Defend what you create

Installation Manual

© Doctor Web, 2015. All rights reserved

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Enterprise Security Suite
Version 10.0
Installation Manual
23.11.2015

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1: Welcome to Dr.Web® Enterprise Security Suite 6

1.1. Introduction 6

1.2. Conventions and Abbreviations 7

1.3. About Product 8

1.4. System Requirements 14

1.5. Distribution Kit 18

1.6. Licensing 19

Chapter 2: Installation of Dr.Web Enterprise Security Suite Components 21

2.1. Planning the Structure of an Anti-Virus Network 21

2.2. Installing Dr.Web Server 21

2.2.1. Installing Dr.Web Server for Windows® OS 22

2.2.2. Installing Dr.Web Server for UNIX® System-Based OS 27

2.2.3. Installing Dr.Web Server Extra Distribution Kit 28

2.2.4. Installing Dr.Web Security Control Center Extension 28

2.3. Installing Dr.Web Agent 30

2.3.1. Installation Files 31

2.3.2. Local Installation of Dr.Web Agent 32

2.3.3. Remote Installation of Dr.Web Agent under Windows® OS 39

2.4. Installing NAP Validator 50

2.5. Installing Proxy Server 50

Chapter 3: Removal of Dr.Web Enterprise Security Suite Components 53

3.1. Removing Dr.Web Server 53

3.1.1. Removing Dr.Web Server for Windows® OS 53

3.1.2. Removing Dr.Web Server for UNIX® System-Based OS 53

3.2. Removing Dr.Web Agent 55

3.2.1. Removing Dr.Web Agent for Windows® OS 55

3.2.2. Removing Dr.Web Agent through Active Directory 57

3.3. Removing Proxy Server 57

Chapter 4: Updating Dr.Web Enterprise Security Suite Software and Its Components 58

4.1. Upgrading Dr.Web Server for Windows® OS 58

4.2. Upgrading Dr.Web Server for UNIX® System-Based OS 61

4.3. Upgrading Dr.Web Security Control Center Extension 65

4.4. Upgrading Dr.Web Agent 65

4.4.1. Upgrading Dr.Web Agents on Stations under Windows® OS 66

4.4.2. Upgrading Dr.Web Agents on Stations under Linux, Android OS X 67

4.5. Upgrading Proxy Server 67

Index 69

Chapter 1: Welcome to Dr.Web® Enterprise Security Suite

1.1. Introduction

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator is intended to introduce general features and provide detailed information on the organization of the complex anti-virus protection of corporate computers using **Dr.Web® Enterprise Security Suite**.

Documentation of **Dr.Web® Enterprise Security Suite** anti-virus network administrator contains the following parts:

1. **Installation Manual** (the **drweb-esuite-10-install-manual-en.pdf** file)

   Installation Manual will be useful to the organization manager who makes the decision to purchase and install a system of comprehensive anti-virus protection.

   Installation Manual explains how to build an anti-virus network and install its general components.

2. **Administrator Manual** (the **drweb-esuite-10-admin-manual-en.pdf** file)
3. **Appendices** (the **drweb-esuite-10-appendices-en.pdf** file)

Administrator documentation contains cross-references between three mentioned documents. If you download these documents to the local computer, cross-references work only if documents are located in the same folder and have their initial names.

Administrator documentation does not include the description of **Dr.Web** anti-virus packages for protected computers. For relevant information, please consult **User Manuals** of **Dr.Web** anti-virus solution for corresponding operating system.

Before reading these document make sure you have the latest version of the Manuals. The Manuals are constantly updated and the current version can always be found at the official web site of **Doctor Web** at http://download.drweb.com/esuite/.

1.2. Conventions and Abbreviations

Conventions

The following conventions are used in the Manual.

Table 1-1. Conventions

Symbol	Comment
Note, that	Marks important notes or instructions.
Warning	Warns about possible errors.
Dr.Web Scanner	Names of **Dr.Web** products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples, input to the command line and application output.
Appendix A	Cross-references or Internal Hyperlinks to web pages.

Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

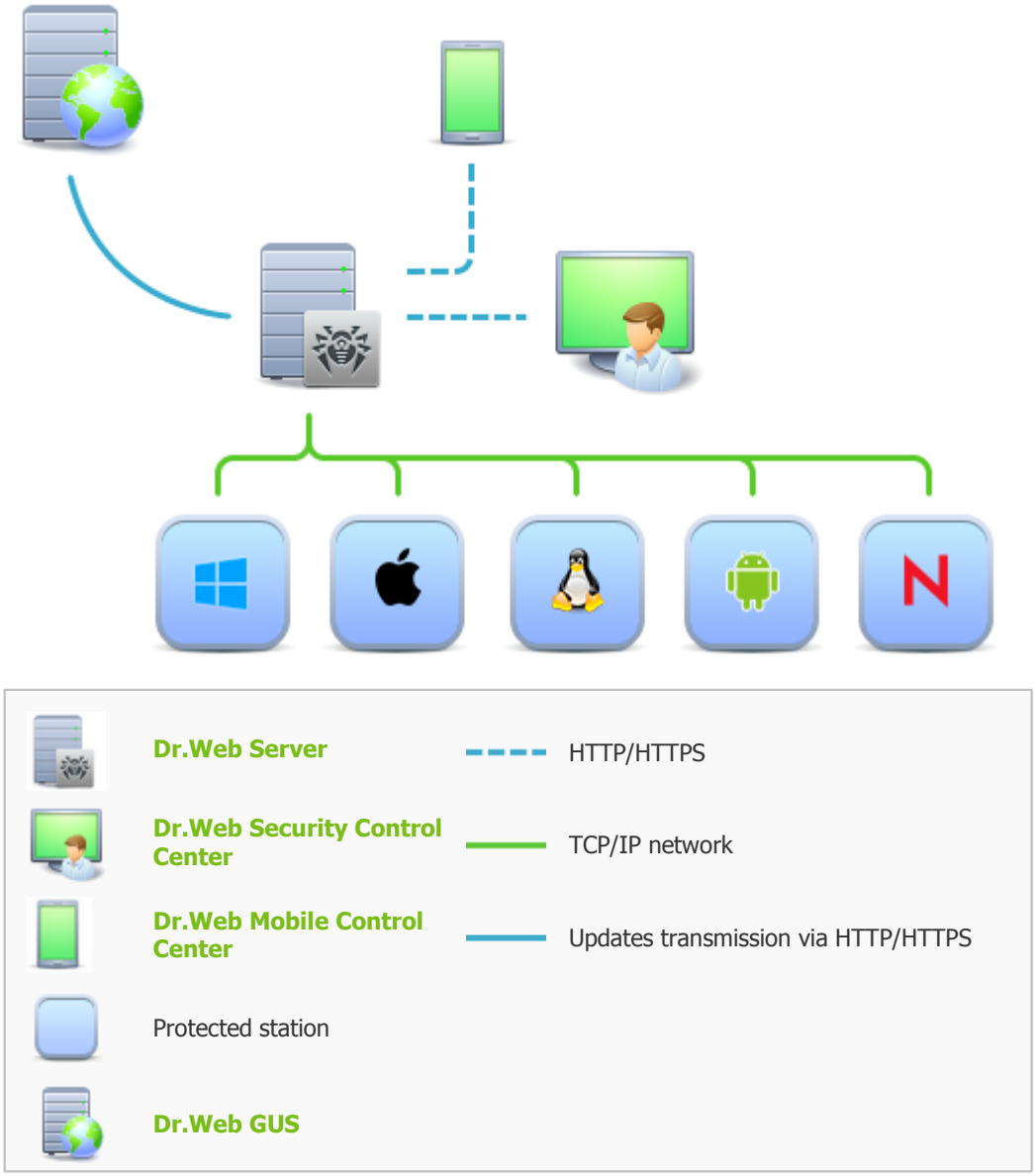
- ACL – Access Control List,
- CDN – Content Delivery Anti-virus network,
- DB, DBMS – Database, Database Management System,
- DFS – Distributed File System,
- DNS – Domain Name System,
- **Dr.Web GUS** – **Dr.Web Global Update System**,
- EBNF – Extended Backus-Naur Form,
- GUI – Graphical User Interface, a GUI version of a program – a version using a GUI,
- LAN – Local Area Network,
- MTU – Maximum Transmission Unit,
- NAP – Network Access Protection,
- OS – operating system,
- PC – personal computer,
- TTL – Time To Live,
- UDS – UNIX domain socket.

1.3. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either local company network including mobile devices, or home computers of employers.

An aggregate of computers and mobile devices on which **Dr.Web Enterprise Security Suite** cooperating components are installed, represents a single *anti-virus network*.

Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on a computers and mobile devises of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP network protocols. Anti-virus software can be installed (and manage them afterwards) on protected stations either via the LAN, or via the Internet.



The logical structure of the anti-virus network

Central Protection Server

Central protection **Server** is installed on a computer of anti-virus network, and installation can be performed on any computer, not only on that functioning as a LAN server. General requirements to this computer are given in the System Requirements section.

Cross-platform **Server** software allows to use a computer under the following operating systems as a **Server**:

- Windows® OS,
- UNIX® system-based OS (Linux®, FreeBSD®, Solaris™).

Central protection **Server** stores distribution kits of anti-virus packages for different OS of protected computers, updates of virus databases and anti-virus packages, license keys and package settings of protected computers. **Server** receives updates of anti-virus protection components and virus databases via the Internet from the **Global Update System** and propagate updates on protected stations.

Hierarchical structure of several Servers can be established to serve protected stations of anti-virus network.

Server supports the backup of critical data (databases, configuration files, etc.).

Server writes single log of anti-virus network events.

Single Database

The single database is connected to the central protection **Server** and stores statistic data on anti-virus network events, settings of the **Server** itself, parameters of protected stations and anti-virus components, installed on protected stations.

You can use the following types of databases:

Embedded database. Two variants of database that is inbuilt into the central protection **Server** directly are provided:

- SQLite2 (InitDB),
- SQLite3.

External database. Inbuilt drivers for connecting the following databases are provided:

- Oracle,
- PostgreSQL,
- ODBC driver to connect other databases such as Microsoft SQL Server/Microsoft SQL Server Express.

You can use any database that corresponds to your demands. Your choice should be based on the needs that must be satisfied by the data store, such as: capability to service the anti-virus network of corresponding size, features of database software maintenance, administration capabilities provided by the database itself and also requirements and standards which are accepted for use in your company.

Central Protection Control Center

Central protection **Control Center** is automatically installed with the **Server** and provides the web interface for remote managing of the **Server** and the anti-virus network by means of editing the settings of the **Server** and protected computers settings stored on the **Server** and protected computers.

The **Control Center** can be opened on any computer that have the network access to the **Server**. The **Control Center** can be used almost under any operating system with full use on the following web browsers:

- Windows® Internet Explorer®,
- Mozilla® Firefox®,

- Google Chrome®.

The list of possible variants of use is given in the System Requirements section.

Central protection **Control Center** provides the following features:

- Serviceability of **Anti-virus** installation on protected stations including: remote installation on protected stations under Windows OS with preliminary browsing the network to search computers; Creation of distribution files with unique identifiers and parameters of connection to the **Server** to facilitate **Anti-virus** installation process by the administrator or possibility of **Anti-virus** installation by users on stations by oneself (detailed information see in the Installing Dr.Web Agent section).
- Facilitate administering based on grouping of anti-virus network workstations.
- Feasibility of centralized administrating of stations anti-virus packages including: uninstallation either separate components or entire **Anti-virus** on stations under Windows OS; configuring parameters of anti-virus package components; assigning permissions to set up and administer the anti-virus packages on protected computers for users of these computers.
- Centralized administering of workstations anti-virus check including: remote launch of anti-virus check either according the specified schedule or direct request from administrator for the **Control Center**; centralized configuration of check parameters and transmitting them to the workstations to launch the local check with these parameters.
- Receiving the statistic information on protected stations states, viral statistics, installed anti-virus software state, running anti-virus components state and also, the list of hardware and software on protected station.
- Flexible administrating system of **Server** and anti-virus network based on opportunity of permissions delimiting for different administrators and also, possibility to connect administrators via the external authorization systems such as Active Directory, LDAP, RADIUS, PAM.
- Managing the licensing of workstations anti-virus protection with branched system of assigning licenses to stations, groups of stations and also, granting licenses between several **Servers** in multiserver configuration of anti-virus network.
- Wide set of setting to configure the **Server** and its separate components including: configuring schedule to maintain the **Server**; plug in user hooks; flexible configuration of update system of all anti-virus network components from the **GUS** and further propagation of updates on stations; configuring the system of administrator notifications about anti-virus network events with different methods of notification delivering; configuring neighbor connections to configure multiserver anti-virus network.

Detailed information on described functions is given in the **Administrator Manual**.

The par of the **Control Center** is the **Web server** that is automatically installed with the **Server**. The general task of the **Web server** is performing operation with web pages of the **Control Center** and clients network connections.

Central Protection Mobile Control Center

As a separate component, the **Mobile Control Center** is provided. It is designed for installation and operation on mobile devices under iOS and Android OS. General requirements to the application are given in the System Requirements section.

Mobile Control Center connects to the **Server** according to the anti-virus network administrator credentials including via an encrypted protocol. **Mobile Control Center** supports the base set of **Control Center** functions:

1. Manage **Dr.Web Server** repository:
   - view the products state in the repository;

- launch repository update from **Dr.Web Global Update System**.

2. Manage stations on which an update of anti-virus software is failed:
   - display failed stations;
   - update components on failed stations.
3. Display statistics information on anti-virus network state:
   - number of stations registered at **Dr.Web Server** and their current state (online/offline);
   - viral statistics for protected stations.
4. Manage new stations waiting for connection to **Dr.Web Server**:
   - approve access;
   - reject stations.
5. Manage anti-virus components installed on anti-virus network stations:
   - launch the fast or full scan either for selected stations or for all stations of selected groups;
   - setup **Dr.Web Scanner** reaction on malware detection;
   - view and manage files in the **Quarantine** either for selected stations or for all stations in the selected group.
6. Manage stations and groups:
   - view properties;
   - view and manage components composition of anti-virus package;
   - delete;
   - send custom messages to stations;
   - reboot stations under Windows OS;
   - add to favorites list for the quick assess.
7. Search for stations and groups in an anti-virus network by different parameters: name, address, ID.
8. View and manage messages on major events in an anti-virus network via the interactive Push notifications:
   - display all notifications at **Dr.Web Server**;
   - set reactions on notification events;
   - search notification by specified filter parameters;
   - delete notifications;
   - exclude notifications from automatic deletion.

You can download **Mobile Control Center** from the **Control Center** or directly in App Store and Google Play.

Network Stations Protection

On protected computers and mobile devices of the network, the control module (**Agent**) and the anti-virus package for corresponding operating system are installed.

Cross-platform software allows to provide anti-virus protection of computers and mobile devises under the following operating systems:

- Windows® OS,
- UNIX® system-based OS,
- OS X®,
- Android OS,
- Novell® NetWare® OS.

Either user computers or LAN servers can be protected stations. Particularly, anti-virus protection of the Microsoft® Outlook® mail system is supported.

Control module performs regular updates of anti-virus components and virus databases from the **Server** and also, sends information on virus evens on protected computer to the **Server**.

If the central protection **Server** is not accessible, it is possible to update virus databases on protected stations via the Internet from the **Global Update System**.

Depending on the operating system of the station, the following protection functions are provided:

Stations under Windows® OS

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** including rootkits check is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Mail monitor

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is is also available (if the license permits this function).

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office control

Controls access to network and local resources, in particular, limits access to web sites. Allows to control the integrity of important files from the accidental change or virus infecting and limit the access to unwanted information for employees.

Firewall

Protects computers from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Self-protection

Protects files and folders of **Dr.Web Enterprise Security Suite** from unauthorized or accidental removal and modification by user or malicious software. If self-protection is enabled, access to files and folders of **Dr.Web Enterprise Security Suite** is granted to **Dr.Web** processes only.

Preventive protection

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocks them in case of detection of viral activity.

Stations under UNIX® system-based OS

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Stations under OS X®

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Mobile devices under Android OS

Anti-virus check

Scans a mobile device on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the **Control Center** is supported.

File monitor

The constant file system protection in the real-time mode. The check of all files as they are saved in the memory of the device.

Calls and SMS Filter

Filtering the incoming phone calls and SMS allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detect the device location or lock its functions in case it has been lost or stolen.

Restricting Internet Access

URL filter allows to protect user of the mobile device from unsolicited Internet sites.

Firewall

Protects the mobile device from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Security Troubleshooting

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

Application launch control

Blocks the launch on mobile device those applications that are not included into the list of allowed by administrator.

Servers under Novell® NetWare® OS

Anti-virus check

Scans a computer on user demand and according to the schedule.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Providing a Connection between Anti-virus Network Components

To provide stable and secure connection between anti-virus network components, the following features are presented:

Dr.Web Proxy server

Proxy server can optionally be included into the anti-virus network. The main function of the **Proxy server** is to provide connection between the **Server** and protected stations in cases when direct connection is impossible. E.g. if the **Server** and protected stations are located in different networks which do not have packet routing between them. At the expense of using caching function, reducing of network traffic and time of receiving updates by protected stations can be provided.

Traffic compression

Special compression algorithms are applicable for transferring data between the anti-virus network components to reduced network traffic to minimum.

Traffic encryption

Data transferred between the anti-virus network components can be encrypted to provide additional secure level.

Additional Features

NAP Validator

NAP Validator is provided as a separate component and allows to use Microsoft Network Access Protection (NAP) technology to check health of protected stations software. The resulting security is achieved through the implementation of the requirements for performance of network stations.

Repository loader

Dr.Web Repository loader is provided as a separate utility and allows to download products of **Dr.Web Enterprise Security Suite** from the **Global Update System**. It can be used for downloading of **Dr.Web Enterprise Security Suite** products updates to place them on the **Server** not connected to the Internet.

1.4. System Requirements

For Dr.Web Enterprise Security Suite to be installed and function the following is required:

- **Dr.Web Server** should be installed on a computer that have an access to the Internet to receive updates from **Dr.Web GUS** (Global Update System) automatically;

It is allowed to propagate updates by any other way to the **Servers** which are not connected to the Internet. Particularly, in multiserver configuration of anti-virus network, it is possible to receive updates from the **GUS** by only one **Server** with subsequent distribution to other **Servers**, or to use **Dr.Web Repository Loader** additional utility to download updates from the **GUS** with subsequent distribution to **Servers**.

- anti-virus network computers should have access to **Dr.Web Sever** or to the **Proxy server**;
- for interaction between the anti-virus components, the following ports must be opened on used computers:

Port numbers	Protocols	Connection directions	Purpose
2193	TCP	• incoming, outgoing for the **Server** and **Proxy server** • outgoing for the **Agent**	For connection between the **Server** and anti-virus components and for interserver communications. Also is used by **Proxy server** to establish a connection with clients.
	UDP	incoming, outgoing	For the **Network Scanner**.
139, 445	TCP	• incoming for the **Server** • incoming, outgoing for the **Agent** • outgoing for the computer on which the **Control Center** is opened	For the **Network Installer**.
	UDP	incoming, outgoing	
9080	HTTP	• incoming for the **Server** • outgoing for the computer on which the **Control Center** is opened	For **Dr.Web Security Control Center**.
9081	HTTPS		
10101	TCP		For **Server** remote diagnostic utility.
80	HTTP	outgoing	For receiving updates from **GUS**.
443	HTTPS		

The 2371 port is required for connection (via TCP and UDP protocols) between components of **4.XX** version. It is used for support of compatibility, particularly during upgrade of anti-virus network components.

Dr.Web Server requires:

Component	Requirement
CPU and operating system	The following operating systems installed on a computer with corresponding CPU are supported: ◆ CPU that supports SSE2 instructions and has 1,3 GHz or faster clock frequency: • Windows; • Linux; • FreeBSD; • Solaris x86. ◆ V9 UltraSPARC IIIi CPU or later: • Solaris Sparc. Complete list of supported OS see in the **Appendices** document, in Appendix A.
RAM	• Minimal requirements: 1 GB. • Recommended requirements: 2 GB and more.
Free disk space	Up to 12 GB: up to 8 GB for a embedded database (installation catalog) and up to 4GB for the system temporary catalog (for work files). Depending on the **Server** settings, additional space may required to store temporary files, e.g. to store personal installation packages of **Agents** (app. 8,5 MB for each) in the `var\installers-cache` subfolder of **Dr.Web Server** installation folder.

Component	Requirement
	To install the **Server**, it is required on Windows OS system disk or in the `/var/tmp` for UNIX system-based OS (or in the other temporary files folder, if it is redefined), not dependently on the **Server** installation folder, at least 1,2 GB for the general distribution kit and 2,5 GB for the extra distribution kit of free system disk space to launch the installer and unpack temporary files.
Other	For the installation of **Dr.Web Server** for UNIX system-based OS, the following libraries required: `lsb` v. `3` or later, `glibc` v. `2.7` and later. To use **PostgreSQL** DB, the `libpq` required. To use **Oracle** DB, the `libaio` required. Additionally under **FreeBSD** OS, the `compat-8x` library required.

Dr.Web Proxy Server requires:

Component	Requirement
CPU	Intel® Pentium® III 667 MHz or faster
RAM	not less than 1 GB.
Free disk space	not less than 1 GB.
Operating system	• Windows; • Linux; • FreeBSD; • Solaris. Complete list of supported OS see in the **Appendices** document, in Appendix A.
Other	For the installation of **Proxy Server** for UNIX system-based OS: `lsb` v. `3` or later. Additionally under **FreeBSD** OS, the `compat-8x` library required.

Dr.Web Security Control Center requires:

- Windows Internet Explorer 8 and later, Mozilla Firefox 25 and later or Google Chrome 30 and later web browsers.

Opera® 10 and later, Safari® 4 and later web browsers also can be used. But operating under these web browsers is not guaranteed.

Full operability of the **Control Center** under Windows Internet Explorer 8 web browser with the *Enhanced Security Configuration for Windows Internet Explorer* mode enabled is not guaranteed.

If you install **Server** on a computer with a '_' (underline) character in the name, configuration of **Server** with **Dr.Web Security Control Center** by use of Windows Internet Explorer will not be available.

In this case, use other web browser.

For proper operation of **Control Center** in Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed **Dr.Web Server** must be added to the trusted sites of browser, on which you open **Control Center**.

For proper opening of **Control Center** via the **Start** menu in Microsoft Internet Explorer browser under Windows 8 and Windows Server 2012 OS with tiled interface, set the following parameters of a web browser: **Tools** → **Programs** → **Opening Internet Explorer** set the **Always in Internet Explorer** flag.

- **Dr.Web Security Control Center** extension to use **Dr.Web Security Control Center** in full. The extension is distributed with the **Server** installation package. It installs by browser request when you use elements of **Dr.Web Security Control Center** which require the extension (for instance, for anti-virus components remote updater or **Network Scanner**). The extension can be installed on Windows Internet Explorer 8 and later or Mozilla Firefox 25 and later web browsers.

For operation of **Dr.Web Security Control Center** extension at the **Network Scanner** page, under both Windows and GNU/Linux OS, you must have administrator (root) rights.

Under Mozilla Firefox web browser, **Dr.Web Security Control Center** extension is available under Windows OS and Linux system-based OS only.

- Recommended screen resolution to use **Dr.Web Security Control Center** is 1280x1024 pt.

Dr.Web Mobile Control Center requires:

Requirements are differ depending on the operating system on which the application is installed:

- iOS:

Component	Requirement
Operating system	iOS® 7 and later
Device	Apple® iPhone® Apple® iPad®

- Android OS:

Component	Requirement
Operating system	Android 4.0 and later

The NAP requires:

For Server

- Windows Server® 2008 OS.

For the Agents

- Windows XP SP3 OS, Windows Vista OS, Windows Server 2008 OS.

Dr.Web Agent and the full anti-virus package require:

Requirements are differ depending on the operating system on which anti-virus solution is installed (the full list of supported OS see in the Appendix A. The Complete List of Supported OS Versions):

- Windows OS:

Component	Requirement
CPU	1 GHz CPU or faster.
Free RAM	Not less than 512 MB.
Free disk space	1 GB for executable files + extra disk space for logs and temporary files.
Other	1. **Dr.Web Agent for Windows** context help requires Windows® Internet Explorer® 6.0 or later. 2. For **Dr.Web for Outlook** extension the the Microsoft Outlook client from the Microsoft Office package is required: ◆ Outlook 2000 (Outlook 9),

Component	Requirement
	◆ Outlook 2002 (Outlook 10 or Outlook XP), ◆ Office Outlook 2003 (Outlook 11), ◆ Office Outlook 2007 (Outlook 12), ◆ Office Outlook 2010 (Outlook 14), ◆ Office Outlook 2013 (Outlook 15).

- Linux system-based OS:

Component	Requirement
CPU	32-bit (IA-32, x86) and 64-bit (x86-64, x64, amd64) Intel platforms.
Free RAM	Not less than 512 MB.
Free disk space	Not less than 400 MB of free disk space on a volume on which **Anti-virus** folders are placed.

- OS X: configuration requirements coincide with the requirements for operating system;
- Android OS: configuration requirements coincide with the requirements for operating system;
- Novell NetWare OS: configuration requirements coincide with the requirements for operating system.

No other anti-virus software (including other versions of **Dr.Web** anti-virus programs) should be installed on the workstations of an anti-virus network managed by **Dr.Web Enterprise Security Suite**.

Functionality of **Agents** is described in the user manuals for corresponding OS.

1.5. Distribution Kit

The program software is distributed depending on the OS of the selected Dr.Web Server:

1. For UNIX system-base OS - as `run` files for installation under corresponding OS versions of the following components:
   - **Dr.Web Server** general distribution kit,
   - **Dr.Web Server** extra distribution kit,
   - **Proxy Server**.
2. For Windows OS - as installation wizard executable files for installation of the following components:
   - **Dr.Web Server** general distribution kit,
   - **Dr.Web Server** extra distribution kit,
   - **Proxy Server**,
   - **Dr.Web Agent** for Active Directory,
   - Utility for Active Directory scheme modification,
   - Utility to change attributes for Active Directory objects,
   - **NAP Validator**.

Dr.Web Server distribution kit contains two packages:

1. *General distribution kit* - basic distribution kit to install **Dr.Web Server**. Composition is similar to composition of previous versions of **Dr.Web Enterprise Security Suite** distribution.

General distribution kit performs the installation of **Dr.Web Server** itself and includes anti-virus protection packages for stations under Windows OS only.

2. *Extra distribution kit* - includes distributions of all enterprise products, which are provided for installation on protected stations under all supported OS.

   The package is installed as an additional on a computer with **Dr.Web Server** *general distribution kit* installed.

Extra distribution kit must be installed from the same type of package as a general distribution kit.

Dr.Web Server general distribution kit contains the following components:

- **Dr.Web Server** software for the respective OS,
- **Dr.Web Agents** software and anti-virus packages software for supported OSs,
- **Dr.Web Security Control Center** software,
- Virus databases,
- **Dr.Web Security Control Center** extension,
- **Dr.Web Server FrontDoor** extension,
- Manuals, templates, and examples.

In addition to the distribution kit, serial numbers are also supplied. Having registered these serial numbers one can get files with a **Server** key and an **Agent** key.

1.6. Licensing

Rights to use **Dr.Web Enterprise Security Suite** are regulated by the license key file.

Key files have a write-protected format based on the mechanism of electronic signature. Editing the file makes it invalid. Therefore it is not recommended to open your key file with a text editor, which may occasionally corrupt it.

Dr.Web Enterprise Security Suite license parameters and price depend on the number of protected computers, which includes the servers protected by **Dr.Web Enterprise Security Suite** network.

Before purchasing a license for a **Dr.Web Enterprise Security Suite** solution you should carefully consider this information and discuss all the details with your local distributor. The number of **Dr.Web Servers** running the network does not affect the license price.

Licensing specific and key files management for already deployed anti-virus network are described in details in **Administration Manual**, p. License Manager.

When purchasing a license for **Dr.Web Enterprise Security Suite** anti-virus, you receive registration keys or a registration card with a serial number.

License key files are generally sent to users by e-mail, after the product serial number has been registered at the special web site: http://buy.drweb.com/register/ unless otherwise specified in the registration card attached to the product. Visit the web site above, in the form enter your personal data and in the corresponding field type the registration serial number (it is written on the registration card). An archive with key files will be sent to the designated address. Or you will be allowed to download it directly from the web site.

As a rule, key files come in a zip-archive, which contains key files for the **Server** and for workstations.

Users can receive key files in one of the following ways:

- by e-mail (usually after registration of the serial number at the web site, see above);
- with the anti-virus distribution kit if license files were included at kitting;
- as a file on a separate carrier.

Please keep key files until they expire. They are required during the installation and re-installation of the anti-virus, as well as to restore program components. In case a license key file is lost, you need to complete the registration form at the web site specified above so that you can restore it. Note that you will need to enter the same registration serial number and the same personal data as during the first registration, you can change the e-mail address only. In this case the license key file will be sent to the new address.

To try the **Dr.Web Enterprise Security Suite** anti-virus and familiarize yourself with the software, you can order demo keys. Such key files provide for the full functionality of the main anti-virus components, but have a limited term of use. Demo key files are sent upon request made through the web form at https://download.drweb.com/demoreq/biz/. Your request for demo keys will be examined and, if approved, an archive with key files will be sent to the designated address.

The use of obtained key files during the installation is described in p. Installing Dr.Web Server.

Chapter 2: Installation of Dr.Web Enterprise Security Suite Components

2.1. Planning the Structure of an Anti-Virus Network

To create an anti-virus network:

1. Make a plan of the anti-virus network structure taking including all protected computers and designating which ones are to function as the **Servers**.
2. Install **Dr.Web Server** software on the selected computer or computers (**Dr.Web Security Control Center** is installed with it).
3. Via the **Control Center**, update the product software in the **Server** repository.
4. Configure the **Server** (**Servers**) and workstations software.
5. Install and configure the **Proxy Server**, if necessary.
6. Install **Dr.Web Agent** software on workstations and then register the anti-virus workstations at **Dr.Web Server**.

Agents establish a connection with the **Server** immediately after the installation. Anti-virus workstations are authorized at the **Server** according to the set policy (see **Administrator Manual**, p. New Stations Approval Policy).

7. Through **Dr.Web Security Control Center**, set up and run the necessary modules.

When planning the structure of the anti-virus network, you should first of all select a computer to perform the functions of **Dr.Web Server**.

Dr.Web Server can be installed on any computer of the local network, not only on that functioning as a local network server. General system requirements to this computer are described in p. System Requirements.

Dr.Web Security Control Center can be opened on any computer, not just on the one with **Dr.Web Server** installed. There should be a network connection with a computer on which the **Server** is installed.

The anti-virus network can incorporate several **Dr.Web Servers**. The features of such configuration are described in **Administrator Manual**, p. Peculiarities of a Network with Several Dr.Web Servers.

To install the **Server** and **Dr.Web Agent**, one-time access (physical or remote) to the correspondent computers is required. All further steps will be taken from the administrator's workplace (which can also be outside the local network) and will not require access to **Dr.Web Servers** and workstations.

2.2. Installing Dr.Web Server

The installation of **Dr.Web Server** is the first step in the installation of **Dr.Web Enterprise Security Suite** anti-virus. Unless and until it is successfully installed, no other **Dr.Web Enterprise Security Suite** components can be installed.

Installation of full package of Dr.Web Server contains the following two steps:

1. Installation of *general distribution kit*. General distribution kit performs the installation of **Dr.Web Server** itself and includes anti-virus protection packages for stations under Windows OS only.

2. Installation of *extra distribution kit*. Extra distribution kit includes distributions of all enterprise products, which are provided for installation on protected stations under all supported OS. The package is installed as an additional on a computer with **Dr.Web Server** general distribution kit installed.

The installation procedure of **Dr.Web Server** depends on **Server** version (for Windows OS or for UNIX system-based OS).

All parameters set during the installation can be changed later by an anti-virus network administrator.

If the **Server** software is already installed on your computer, see the Upgrading Dr.Web Enterprise Security Suite for Windows® OS or Upgrading Dr.Web Enterprise Security Suite for UNIX® System-Based Systems sections correspondingly.

If the previously installed **Server** was removed before installing the **Server** software, contents of the repository will be deleted during installation and the new version will be installed. If the repository of the previous version by some reason was not removed, it is necessary to manually delete the contents of the repository before installing the new version of the **Server** and then renew the repository after installation.

The language for the **Server** installation folder name must match to the language, specified in language settings of Windows OS for the non-Unicode programs. In opposite case, the **Server** will not be installed.

The english language is an exception for the installation folder name.

Together with **Dr.Web Server**, **Dr.Web Security Control Center** is installed, which serves to manage the anti-virus network and set up the **Server**.

By default, **Dr.Web Server** will run automatically after the installation under Windows OS and must be started manually under UNIX system-based OS.

2.2.1. Installing Dr.Web Server for Windows® OS

Below is described the installation of **Dr.Web Server** for Windows OS. The set and the order of steps may somewhat differ depending on the distribution file version.

Before installing, please consider the following:

The distribution file and other files requested during the program installation should reside on local drives of the computer on which the **Server** software is installed; these files should be made accessible for the LocalSystem user.

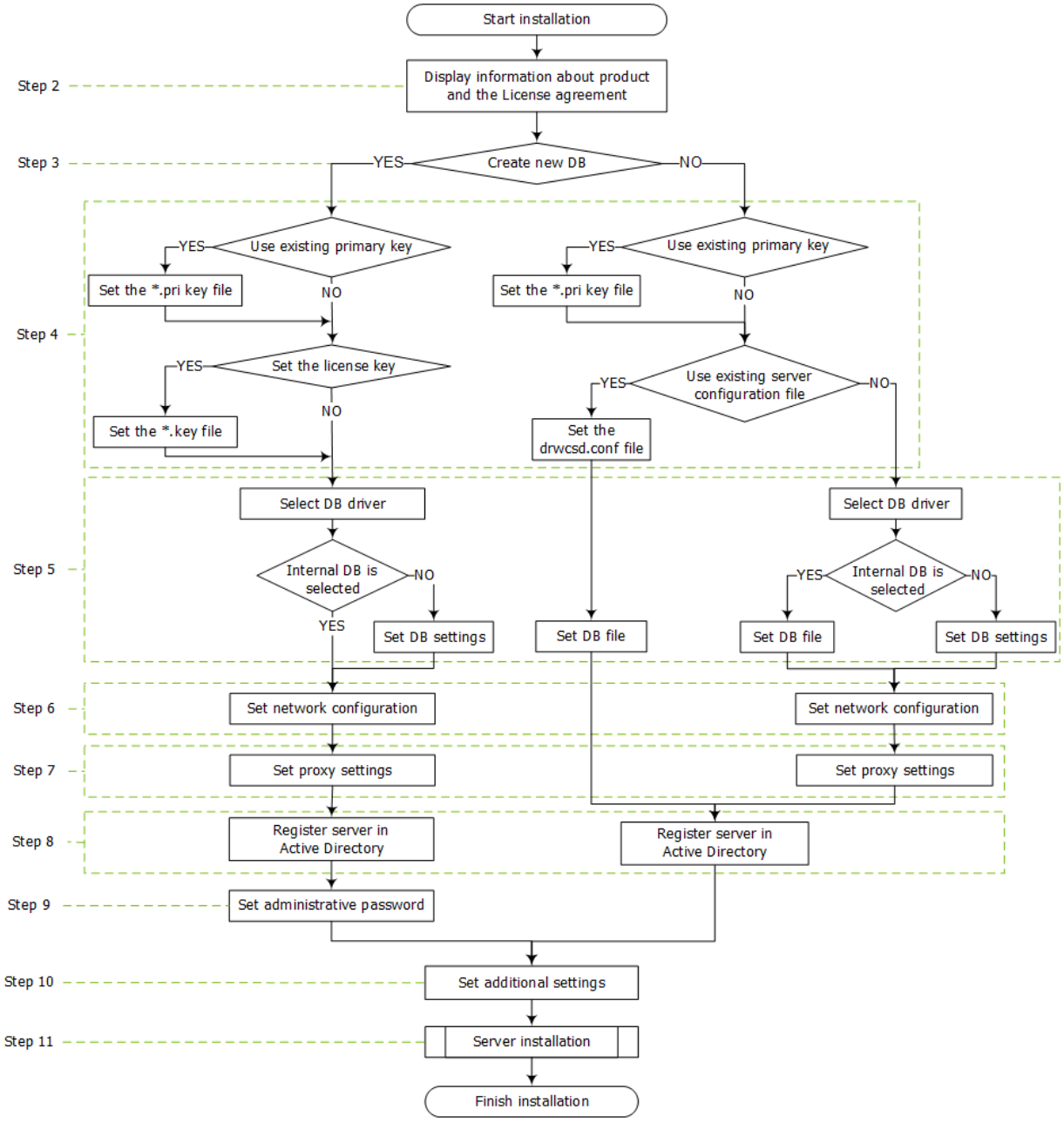
Dr.Web Server should be installed by a user with the administrator's rights to the computer.

After **Dr.Web Server** is installed it is necessary to update all **Dr.Web Enterprise Security Suite** components (see **Administrator manual**, p. Manual Updating of Dr.Web Enterprise Security Suite Components).

In case an external database is to be used it is necessary to create the database first and set the ODBC driver (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).

Server installation module supports the product change mode. To add or remove separate components, e.g. database configuration drivers it is necessary to run the **Server** installer and select **Change**.

Figure 2-1 illustrates the flowchart of **Dr.Web Server** installation procedure. Steps in the flowchart correspond with the detailed description of the installation procedure shown below.



Picture 2-1. Dr.Web Server installation procedure flowchart (click any block in the flowchart to see its description)

To install Dr.Web Server on a computer operated by Windows OS:

1. Run the distribution file.

By default, installer uses the language of the operating system. If necessary, you can change the installation language on any step by selecting the corresponding option in the right upper part of the installer window.

2. A window with information on the product to install and the link to the license agreement text will be opened. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
3. In the next window, select which database will be used for the anti-virus network:

- **Create a new database** - to create a new anti-virus network.
- **Use the existing database** - to keep the database from the previous **Server** installation. You will be able to specify the database file later (see step **5**).

4. In the next window, setup the database.

a) If at step **3** you have selected the **Create a new database** option, in the **New Database Parameters** window, specify the following settings:

- The **Set the license key** flag allows to set **Dr.Web Agent** license key file during the **Server** installation.
  - If the flag is cleared, the **Server** installation is performed without the **Agent** license key. In this case, the license keys must be added after the **Server** installation via the License Manager.
  - If the flag is set, you must specify the path to the **Agent** license key file in the corresponding field.
- The **Use existing private encryption key** flag allows to use the existing encryption keys, e.g., from the previous **Server** installation.
  - At the first **Server** installation, clear the **Use existing private encryption key** flag. The new encryption keys will be automatically generated during the installation process.
  - If you are installing the **Server** for an existing anti-virus network, set the **Use existing private encryption key** flag and specify the path to the private key file in the corresponding field. At this, the public key file will be automatically generated (content of the public key will match the content of the previous public key). This allows for already installed **Agents** to connect to the new **Server**. Otherwise, after the installation, it will be necessary to copy the new public encryption key to all workstations, on which **Dr.Web Agents** have been previously installed.
    If an error occurs during the public key extraction, specify the path to the file with the corresponding public key manually in the **Specify public encryption key** opened field.

For evaluation purposes, you can use a demo key files. Click **Request the demo key** to go to the official web site of **Doctor Web** company and receive the demo license key files (see Demo key files).

b) If at step **3** you have selected the **Use the existing database** option, in the **Existing Database Parameters** window, specify the following settings:

- The **Use existing configuration file** flag allows to specify the **Server** settings.
  - If the flag is cleared, the **Server** configuration file with the default settings will be created.
  - If the flag is set, you must specify the path to the configuration file with the **Server** settings in the corresponding field.
- The **Use existing private encryption key** flag allows to use the existing encryption keys, e.g., from the previous **Server** installation.
  - At the first **Server** installation, clear the **Use existing private encryption key** flag. The new encryption keys will be automatically generated during the installation process.
  - If you are installing the **Server** for an existing anti-virus network, set the **Use existing private encryption key** flag and specify the path to the private key file in the corresponding field. At this, the public key file will be automatically generated (content of the public key will match the content of the previous public key). This allows for already installed **Agents** to connect to the new **Server**. Otherwise, after the installation, it will be necessary to copy the new public encryption key to all workstations, on which **Dr.Web Agents** have been previously installed.
    If an error occurs during the public key extraction, specify the path to the file with the corresponding public key manually in the **Specify public encryption key** opened field.

For evaluation purposes, you can use a demo key files. Click **Request the demo key** to go to the official web site of **Doctor Web** company and receive the demo license key files (see Demo key files).

5. The **Database Driver** window allows you to adjust the parameters of the used database which depend on the database type specified at step **3** and the availability of the **Server** configuration file specified at step **4.**
   - If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the **Server** configuration file, select the driver to use. At this:
     - The **SQLite (built-in database)** and **IntDB (built-in database)** options prescribe to use built-in facilities of **Dr.Web Server**. Additional parameters are not required.
     - The rest options imply usage of an external DB. You must specify corresponding parameters to configure the access to a DB. Parameters of DBMS are described in the appendices (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).
   - If at step **3** you have selected the **Use the existing database** option and at step **4** you have specified the path to the **Server** configuration file, specify the path to the database file to use according to the specified **Server** configuration file.
6. If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the **Server** configuration file, the **Network Configuration** window will be opened. You can set up a network protocol for the **Server** (it is allowed to specify only one network protocol; additional protocols can be configured later).

   To specify the network settings from the predefined set, select one of the following variants from the drop-down list:

   - **Standard configuration** prescribes to use default settings on base of the **Server** detection service.
   - **Limited configuration** prescribes to limit the **Server** operation only to the internal network interface – `127.0.0.1`. With such settings the **Server** can be administrated only from the **Control Center** opened on the same computer, and communicate only with the **Agent** launched on the same computer. In future, after the **Server** settings have been checked out you will be able to change network settings.
   - **User-defined configuration** indicates what the following predefined setting are changed:
     - In the **Interface** and **Port** fields, specify the corresponding values to access the **Server**. Default interface is `0.0.0.0`, which means that the **Server** can be accessed via any interface.

By default the `2193` port is used.

Note: in **Servers 4.XX** the `2371` port was used. In the **10.0** version this port is no longer supported.

Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

     - Set the **Restrict access to Dr.Web Server** flag to limit the local access to the **Server**. The **Agent Installers**, **Agents** and other **Servers** (for existing anti-virus network built with **Dr.Web Enterprise Security Suite**) will not be able to access the **Server**. You can change these settings later via **Dr.Web Security Control Center** menu **Administration** → **Dr.Web Server configuration** → **Modules** tab.
     - Set the **Enable Dr.Web Server detection service** if you want the **Server** to answer broadcast and multicast requests from other **Servers** by IP address and service name specified in the corresponding fields below.
7. If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the **Server** configuration file, the **Proxy server** window will be opened to setup parameters of a proxy server usage when connecting to the **Server**:

   To connect to the **Server** via the proxy server, set the **Use proxy server** flag.

The **Use proxy server** flag will be available only if the **Server** installation folder does not contain configuration files from the previous installation.

Specify the following parameters to setup a connection to the proxy server:

- **Proxy server address** - the proxy server address (obligatory field),
- **User name**, **Password** - user name and the password to access the proxy server, if the proxy server supports authorized connection.
- In the **Authorization method** drop-down list, select necessary method of authorization at proxy server, if the proxy server supports authorized connection.

8. If computer on which you are installing the **Server** is included into the Active Directory domain, in the next window you will be prompted to register **Dr.Web Server** in the Active Directory domain. During registration in Active Directory domain, the SRV record corresponding to **Dr.Web Server**, is created on DNS server. Further, clients can access **Dr.Web Server** via this SRV record.

   Specify the following parameters for the registration:

   - Set the **Register Dr.Web Server in the Active Directory** flag.
   - In the **Domain** field, specify the name of the Active Directory domain to register the **Server** in. If the domain is not specified, the domain in which the computer with installing **Server** is registered, is used.
   - In the **User name** and **Password** fields, specify Active Directory domain administrator credentials.

9. If at step **3** you have selected the **Create a new database** option, the **Administrative password** window will be opened. Specify the password for anti-virus network administrator which is created by default with the **admin** login and the full set of permissions to manage anti-virus network.
10. The next window notifies you that the Wizard is ready to install **Dr.Web Server**. If necessary, you can configure additional installation parameters. For this, click **Additional parameters** in the bottom if the window and specify the following settings:
    - On the **General** tab:
      - In the **Dr.Web Security Control Center interface language** drop-down list, select default interface language for **Dr.Web Security Control Center**.
      - In the **Dr.Web Agent interface language** drop-down list, select default interface language for **Dr.Web Agent** and anti-virus package components installing on stations.
      - Set the **Share Dr.Web Agent installation folder** flag to change the usage mode and the name of **Agent** shared installation folder (hidden name of shared resource is set by default).
      - Set the **Launch Dr.Web Server after installation is complete** flag to start the **Server** automatically after the installation.
      - Set the **Update repository after installation is complete** flag to update the **Server** repository automatically after the installation is complete.
      - Set the **Send statistics to Doctor Web company** flag to send statistics on virus events to **Doctor Web** company.
    - On the **Path** tab:
      - In the **Dr.Web Server installation folder** field, the folder to install the **Server** is specified. To change default folder, click **Browse** and select the necessary folder.
      - In the **Dr.Web Server backup folder** field, the folder to backup **Server** critical data according to the tasks from the **Server** schedule is specified. To change default folder, click **Browse** and select the necessary folder.
    - On the **Components** tab, you can select the components you want to install.

If you are going to use the ODBC for Oracle as an external database, select the **Custom** option and disable the installation of Oracle client (in the **Database support** - **Oracle database driver** section) in the opened window.

Otherwise, Oracle DB functioning will fail because of the libraries conflict.

- On the **Log** tab, you can specify the settings for logging of the **Server** installation and operation.

After the additional parameters setup is finished, click **OK** to apply these changes or **Cancel** if no changes were made or to cancel specified changes.

11. Click **Install** to start the installation. Further actions of the installation program do not require user intervention.
12. Once the installation is complete, click **Finish**.

As a rule, **Dr.Web Server** can be managed via **Dr.Web Security Control Center** which acts as an interface for the **Server**.

In the **Programs** main menu of Windows OS installation wizard places the **Dr.Web Server** folder containing the following elements for configuration and managing the **Server**:

- The **Server control** folder contains the commands to start, restart and shut down the **Server**, as well as the commands to set up the logging parameters and other **Server** commands described in detail in Appendix H5. Dr.Web Server.
- **Web interface** item opens **Dr.Web Security Control Center** and connects to the **Server** installed at this computer (at the http://localhost:9080).
- **Documentation** item opens administrator documentation in HTML format.

Structure of the **Server** installation folder is described in the **Administrator Manual**, in the Dr.Web Server section.

2.2.2. Installing Dr.Web Server for UNIX® System-Based OS

Installation should be carried out in console under superuser account (**root**).

Package-based installation of Dr.Web Server on a UNIX system-based OS

1. To start installing the **Server**, use the following command:

```
sh ./<distribution_file>.run
```

To launch the installation package, you can use command line switches. Parameters of command line launch are given in the **Appendices** document, p. H10. Dr.Web Server Installer for UNIX® System-Based OS

By default, administrator's name is **admin** and the password is **root**.

2. Next, the text of the license agreement presented. To proceed the installation, you must accept the license agreement.
3. On a request of backup folder, specify the path to the necessary folder or confirm default backup folder - `/var/tmp/drwcs`.
4. If the extra distribution kit is detected in the system, you will be informed about deletion of the extra distribution kit before installation of the **Server** package. You cannot continue the installation without deletion of extra distribution kit.
5. Then the program components will be installed on your computer. In the course of the installation you can be asked to confirm some actions as the administrator.

In the course of the installation of the **Dr.Web Server** for **FreeBSD** OS an `rc` script `/usr/local/etc/rc.d/drwcsd.sh` will be created.

Use the following commands:

- `/usr/local/etc/rc.d/drwcsd.sh stop` - manually stop the **Server**,
- `/usr/local/etc/rc.d/drwcsd.sh start` - manually start the **Server**.

Please note, during the **Server** installation, the license key is not specified. License keys must be added after installation of the **Server**, via the License Manager.

2.2.3. Installing Dr.Web Server Extra Distribution Kit

Installation of extra distribution kit must be performed on a computer with **Dr.Web Server** general distribution kit installed. Description of **Server** general distribution kit installation is given in the Installing Dr.Web Server for Windows® OS and Installing Dr.Web Server for UNIX® System-Based OS sections.

Extra distribution kit must be installed from the same type of package as a general distribution kit.

To install Dr.Web Server extra distribution kit on a computer operated by Windows OS:

1. Run the distribution file.
2. The **Dr.Web ESuite Extra** window with information about the program and the license agreement to be installed will be opened. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Install**.
3. Installation of extra distribution kit begins. If no errors occur, further actions of the installation program do not require user intervention.
4. Once the installation is complete, click **Finish**. Computer reboot is not required.

To install Dr.Web Server extra distribution kit on a computer operated by UNIX system-based OS:

1. Run the distribution file via the following command:

   `sh ./<distribution_file>.run`

2. Next, the text of the license agreement presented. To proceed the installation, you must accept the license agreement.
3. Then the program components will be installed on your computer.

2.2.4. Installing Dr.Web Security Control Center Extension

Under Mozilla Firefox, Opera ans Chrome web browsers, **Dr.Web Security Control Center** extension installation is available under Windows OS and Linux system-based OS only.

Dr.Web Security Control Center extension is required for full functionality of **Dr.Web Security Control Center** (see also the System Requirements section).

The extension is distributed with the **Server** installation package and can be installed:

1. Automatically, by browser request when you use **Dr.Web Security Control Center**, particularly, elements which require the extension (anti-virus components remote updater or **Network Scanner**).
2. Manually, via **Dr.Web Security Control Center** extension installer.

Manually Installation of Dr.Web Security Control Center Extension

To download Dr.Web Security Control Center Extension for manually installation:

1. Open **Dr.Web Security Control Center**. If **Dr.Web Security Control Center** extension for using browser is not installed yet, under the main menu, recommendation on extension installation will be presented.
2. Follow the **Install Dr.Web Security Control Center browser extension** link.

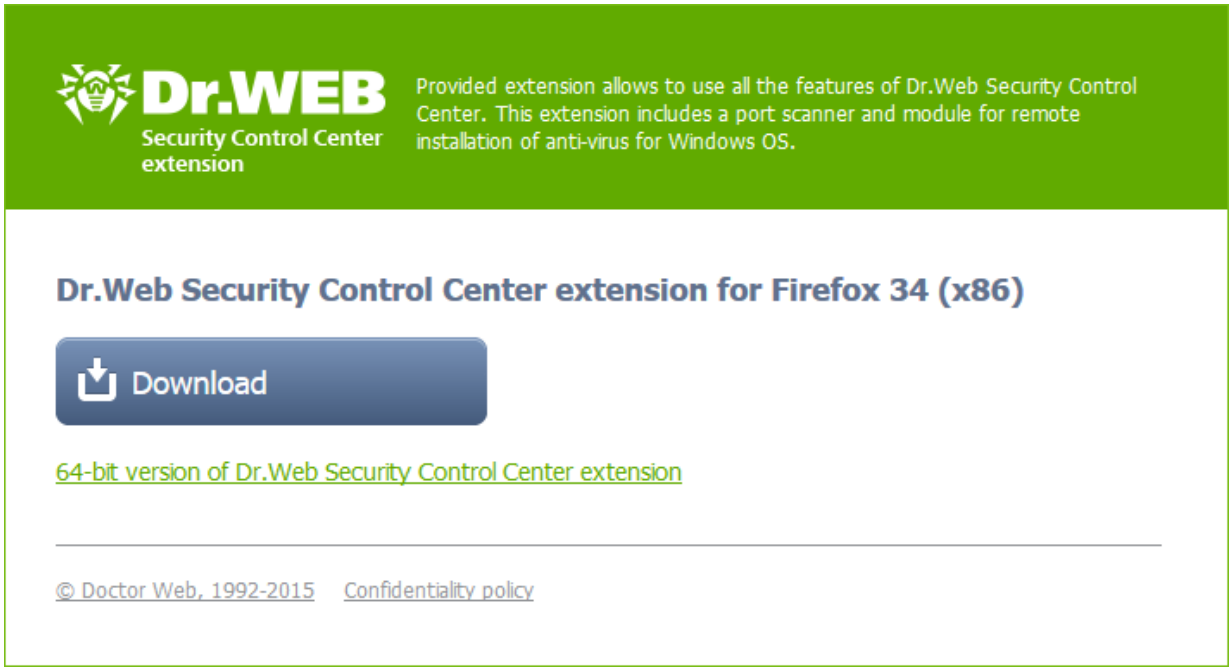

Dr.WEB
Security Control Center extension
Provided extension allows to use all the features of Dr.Web Security Control Center. This extension includes a port scanner and module for remote installation of anti-virus for Windows OS.
Dr.Web Security Control Center extension for Firefox 34 (x86)
Download
64-bit version of Dr.Web Security Control Center extension
© Doctor Web, 1992-2015
Confidentiality policy

Figure 2-2. Section for downloading Dr.Web Security Control Center extension

3. In the extension download section, version of current browser and offered extension bit rate (x86 or x64) are represented.

   For UNIX system-based systems you can select distribution kit for corresponding OS from the drop-down list.

4. To download and save the extension, click **Download**. After this, you can install the extension manually.
5. To change the bit rate of the extension, click the link under download button, after this you can download installer as described at step **4**.

To install Dr.Web Security Control Center Extension under Windows OS:

1. Run the installation file. On the Welcome page of the **InstallShield Wizard**, click **Next**.
2. On the **License Agreement** page, read the agreement. To accept the agreement and proceed with the installation, select **I accept the terms of the license agreement** and click **Next**. To exit the wizard, click **Cancel**.
3. A window for changing the default installation folder will be opened. If necessary, click **Change** and specify the installation folder. Click **Next**.
4. Click **Install**. The installation begins. Further actions of the installation program do not require user intervention.

5. When installation completes, click **Finish**.

To install Dr.Web Security Control Center Extension under UNIX system-based OS:

Execute the following command:

- for **deb** packages:
  `dpkg -i drweb-esuite-plugins-linux-<distribution_version>.deb`
- for **rpm** packages:
  `rpm -i drweb-esuite-plugins-linux-<distribution_version>.rpm`
- for other systems (**tar.bz2** and **tar.gz** packages):
  1. Unpack the archive with browser extension.
  2. Create a directory for browser extensions, if it is not exist.

  For example, for Mozilla Firefox browser: `mkdir /usr/lib/mozilla/plugins`
  3. Copy unpacked at step 1 library to the extensions directory.

  For example, for Mozilla Firefox browser: `cp libnp*.so /usr/lib/mozilla/plugins`

After installation of **Dr.Web Security Control Center Extension** under UNIX system-based OS, restart web browser, if it was started.

2.3. Installing Dr.Web Agent

Dr.Web Agent should be installed under Administrator account of the respective computer.

If **Dr.Web Agent** is installed on the computer, you must uninstall the **Agent** before the installation.

Anti-virus can be installed on a protected workstation in two ways:

1. Locally.

   Local installation is performed directly on the user's computer or mobile device. May be performed either by administrator or by user.

2. Remotely.

   Remote installation is available for stations under Windows OS only and performed in the **Control Center** through the LAN. Performed by the anti-virus network administrator. No user interference required.

Dr.Web Agent installation over Dr.Web standalone product on stations under Windows OS

If a standalone **Dr.Web** product of **7**/**8**/**9** version is installed on the station, the installation of **Agent** for **Dr.Web Enterprise Security Suite** version **10.0** is preformed according to the following scheme:

- If the **Agent** installer or installation package is launched in the GUI mode on the station with standalone product of **7.0**/**8.0**/**9.0** version installed, the installer of corresponding version of installed product will be launched. After this, the user is prompted to enter the confirmation code and uninstall the product. After the OS reboot, the GUI version of **Agent** installer for **Dr.Web Enterprise Security Suite** version **10.0** is launched.
- If the **Agent** installer is launched in the background mode on a station with standalone product of **7.0**/**8.0**/**9.0** version installed, this will not incur any actions. In case of remote installation, the installer returntsthe message to the **Control Center** about standalone product of previous version installed. In this case, you must remove standalone product manually and install the **Agent** for **Dr.Web Enterprise Security Suite** version **10.0** by any of available ways.

- If the **Agent** installer is launched on a station with standalone product of **9.1** version, the installed product switches from the standalone mode to the centralized protection mode. After connection and authorization on the **Server**, the updates, new settings and the list of installing components can be received, depending on which, reboot may required.

For installation of Dr.Web Agent on LAN servers and cluster computers, consider the following:

- For installation on computers which implement terminal servers functions (the **Terminal Services** are installed on Windows OS), to provide **Agents** operation in user's terminal sessions, **Agents** software must be installed locally, via the Add or Remove Programs Wizard on **Control Panel** of Windows OS.
- It is not recommended to install **SpIDer Gate**, **Office Control**, **SpIDer Mail** and **Dr.Web Firewall** components on servers which implement significant network functions (domain controllers, license distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** anti-virus.
- Installation of the **Agent** on a cluster must be performed separately on each cluster node.
- The operation principles for **Agents** and anti-virus package on the cluster node are similar to those on a standard LAN server, thus, it is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on cluster nodes.
- If access to quorum resource of a cluster is severely restricted, it is recommended to exclude it from the scan by the **SpIDer Guard** and confine by regular checks of the resource via **Scanner** launched by scheduler or manually.

2.3.1. Installation Files

Personal Installation Package

After a new stations account is created in the **Control Center**, a personal installation package for **Dr.Web Agent** installation is generated. Personal installation package contains **Dr.Web Agent** installer and the set of parameters for connecting to the **Server** and for authorization of the station at the **Server**.

Personal installation packages are available for protected stations under all operating systems which are supported by **Dr.Web Enterprise Security Suite**. At this:

- For stations under Windows OS, installation package is generated in the **Control Center** in base of **Agent** network installer. Parameters for connecting to the **Server** and for authorization of the station at the **Server** are included into installation packe directly.
- For stations under Android OS, Linux OS, OS X, installation package is an installer for **Dr.Web Agent** installation and configuration file with parameters for connecting to the **Server** and for authorization of the station at the **Server**.

To have installation packages for operating systems other that Windows OS, you must install extra distribution kit of **Dr.Web Server** first.

Download link for **Dr.Web Agent** personal installation package for the concrete station is available:

1. After creating of a new station (see the **11** step in the Creation of a New Station Account section).
2. In any time after station creation:
   - in station properties,
   - in the **Selected objects** section for the station selected in hierarchical list.

Installer

Agent installer differs from the installation package that it does not contain parameters for connecting to the **Server** and for authorization of the station at the **Server**.

The following types of **Dr.Web Agent** installers are provided:

- For stations under Windows OS, two type of installers are available:
  - `drwinst.exe` *Network Installer* performs the installation of the **Agent** only. After connecting ti the **Server**, the **Agent** downloads and installs necessary anti-virus package components. It is possible either local or remote installation of the **Agent** via the network installer.

    The `drwinst.exe` **Agent** network installer resides in the `Installer` folder (the shared hidden resource by default) of **Dr.Web Server** installation folder. Network sharing at the 10 step during **Dr.Web Server** installation is set. You can change this resource further.
  - `drweb-esuite-agent-full-10.00.0-`*<build_version>*`-windows.exe` *Full Installer* performs the installation of the **Agent** and anti-virus package at a time.
- For stations under Android OS, Linux OS, OS X, installers for **Dr.Web Agent** installation similar to the stand-alone version are available.

Dr.Web Agent installers are available on the installation page of **Dr.Web Security Control Center**.

> To have installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of **Dr.Web Server** first.

Installation Page

At the installation page of **Dr.Web Security Control Center** you can download:

1. **Dr.Web Agent** installer.

   Installers for protected stations under all operating systems which are supported by **Dr.Web Enterprise Security Suite** are located in corresponding named folders.

2. The `drwcsd.pub` public encryption key.

From any computer with network access to the **Server**, installation page is available at the following address:
`http://`*<Server_address>*`:`*<port_number>*`/install/`

where *<Server_address>* is the IP address or DNS name of the computer on which **Dr.Web Server** is installed. And the *<port_number>* should be `9080` (or `9081` for https).

2.3.2. Local Installation of Dr.Web Agent

Local installation of **Dr.Web Agent** is performed directly on the user's computer or mobile device. May be performed either by administrator of by user.

> You must update the **Server** repository before the first installation of the **Agent** (see **Administrator manual**, p. Manual Updating of Dr.Web Enterprise Security Suite Components, p. **Checking for Updates**).

Stations under Android OS, Linux OS, OS X

For local installation of **Dr.Web Agent** on stations under Android OS, Linux OS, OS X the following means are available:

- Personal installation package, created in the **Control Center**.
- Installer of **Dr.Web Agent**.

When you choose the type of installing package, please note the following features:

a) When the personal installation package is created, **Dr.Web Agent** installer is provided for installation, and parameters for connecting to the **Server** and for authorization of the station at the **Server** are provided in the configuration file.

b) For installation via the installer, **Dr.Web Agent** is installed, but parameters for connecting to the **Server** and for authorization of the station at the **Server** are not provided.

Stations under Windows OS

For local installation of **Dr.Web Agent** on stations under Windows OS, the following means are available:

- Personal installation package created in the **Control Center**.
- Full installer of **Dr.Web Agent**.
- Network installer of **Dr.Web Agent**.

When you choose the type of installing package, please note the following features:

a) For installation via the personal installation package, parameters for connecting to the **Server** and for authorization of the station at the **Server** are included into the personal installation package. Installation via the personal installation package is performed on base of the network installer from which the **Agent** only is installed. After connecting to the **Server**, the **Agent** downloads and installs the anti-virus package components.

b) For installation via the full installer, the **Agent** and anti-virus package are installed at a time. At this, parameters for connecting to the **Server** and for authorization of the station at the **Server** are not provided.

c) For installation via the network installer, the **Agent** only is installed. After connecting to the **Server**, the **Agent** downloads and installs the anti-virus package components. At this, parameters for connecting to the **Server** and for authorization of the station at the **Server** are not provided.

To have installation packages and installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of **Dr.Web Server** first.

You can also launch all types of the **Agent** installation files from the command line using the switches given in the **Appendices** document, p. H2. Network Installer.

2.3.2.1. Installing Dr.Web Agent via the Personal Installation Package

To install Dr.Web Agent on protected stations via the personal installation package:

1. Via the **Control Center**, create an account for a new station on the **Server**.
2. Send to a user the link on **Dr.Web Agent** personal installation package for corresponding operating system of a computer or mobile device, if a user performs **Dr.Web Agent** software installation directly. If the installation is performed on a station under operating system other than Windows OS, you must also send the configuration file with **Dr.Web Server** connection settings to a user (see step **11** in the Creation of a New User Account procedure).

For easy delivering of installation and configuration files, you can use the **Mailing of installation files** function (detailed information is given in the **Administrator Manual**, p. Mailing of Installation Files) to email messages with corresponding files.

3. Install **Dr.Web Agent** on a workstation.

Local installation of **Dr.Web Agent** on workstations is described in the **User Manual** for corresponding OS.

Dr.Web Agent should be installed by a user with the administrator rights to the computer.

If anti-virus software has already been installed on a workstation, then before starting installation the installer will attempt to remove it. If the attempt fails, the user will have to uninstall the anti-virus software from his computer by himself.

4. Configure parameters of connection to **Dr.Web Server** on a station directly.

Creation of a New Station Account

To create a user account or several user accounts, use **Dr.Web Security Control Center**.

When creating a user account, please note the name of the **Server** specified in the following sections of the **Control Center**:

1. **Administrating** > **Web server configuration** > the **Server** field (stored in the `<server-name />` parameter of the `webmin.conf` configuration file). This parameter value is used when generating the link on the **Agent** installation package.
   If the parameter value is not specified, when the DNS name (if available) or IP address of a computer on which the **Control Center** is opened, is used as a **Server** name to generate the link on **Agent** installer download.
2. **Administrating** > **Dr.Web Server configuration** > the **Download** tab > the **Server** field (stored in the `<name />` parameter of the `download.conf` configuration file). This parameter value is specified in the **Agent** installation packages and defines to which **Server** the **Agent** connects during installation.
   If the parameter value is not specified, when creating an installation package of the **Agent**, the name of the **Server** to which the **Control Center** connected is used. In this case, the **Control Center** must be connected to the **Server** using the IP-address of the domain for which you create an account (the **Server** address must not be specified as a loopback - `127.0.0.1`).

To create a new user via Dr.Web Security Control Center, do the following:

1. Select the **Anti-virus network** item in the main menu of the **Control Center**.

2. In the toolbar, click **Add a station or a group**. In the opened submenu, select the **Create station** option. A pane for the new user account creation will be opened in the right pane of **Dr.Web Security Control Center**.
3. In the **Number** entry field, specify the number of accounts to be created.
4. In the **Identifier** field, unique identifier of created station will be generated automatically. You can edit it, if necessary.
5. In the **Name** field, specify the station name, that will be displayed in the anti-virus network hierarchical list. Further, after the station is connected with the **Server**, this name can be automatically changed to the station name, which is specified locally.
6. In the **Password** and **Retype password** fields you can specify a password for accessing the **Server**. If the password is not specified, it will be generated automatically.

When creating more than one account, **Identifier**, **Name** and **Password** (**Retype password**) fields are set automatically and can not be changed at the stage of station creation.

7. In the **Description** field, specify additional information about the customer. This parameter is optional.
8. In the **Groups** section, specify groups in which the created station will be included.
   - In the **Membership** list, you can configure the list of user groups into which the station will be included.
     By default, station is included into the **Everyone** group. If custom groups are available, you can include creating station into those groups with no limitations on the number of groups into which the station is included. To do this, set the flags next to the user group names in the **Membership** list.

You cannot exclude stations from the **Everyone** group and from a primary groups.

To set a primary group for the creating station, click the icon of the corresponding group from the **Membership** list. The **1** will appear on the group icon.

9. Specify parameters of the **Security** section, if necessary. Parameters of this section are described in the **Administrator Manual**, in the p. Security.
10. Specify parameters of the **Location** section, if necessary.
11. Click **Save** in the upper right corner. The opened pane contains information about successful creation of a station, its ID and the following links:
    - The **Installation file** item contains the link for downloading **Agent** installer for this station.

After a new station has been created, before the operating system of a station is set, in the section of distribution kit downloading, the links are presented separately for all OS that are supported by the **Dr.Web Enterprise Security Suite**.

To have installation packages for operating systems other that Windows OS, you must install extra distribution kit of **Dr.Web Server** first.

    - The **Configuration file** item contains the link for downloading the file with settings of connection to **Dr.Web Server** for stations under Android, OS X and Linux operating systems.
    - The **Password** item contains the password to access the **Server** for this station. To view the password, click .

Link for the **Agent** installation package downloading is also available:

- in station properties after its creation,
- in the **Selected objects** section for the station selected in hierarchical list.

See also the Installation Files section.

- In this window, the **Install** button is also available which is intended for remote installation of Dr.Web Agent Software via Dr.Web Security Control Center.

12. Installation of **Dr.Web Anti-virus** on workstations is described in the **User Manual** for corresponding OS.

Configuring Parameters of Connection to Dr.Web Server

- **Stations under Windows OS**

  After installation of **Dr.Web Agent** on stations under Windows OS via the personal installation package, additional configuring is not required. Parameters of connection to the **Server** and authorization parameters are included into a personal installation package directly. After the **Agent** installation is complete, the station automatically connects to the **Server**.

- **Stations under Android OS**

  1. On the main screen of a mobile device, open **Dr.Web Anti-virus** application menu and select **Settings**.
  2. On the **Dr.Web - Settings** screen on the **Mode** section, set the **Dr.Web Agent** flag.
  3. Parameters of connection to the **Server**, such as IP address and authorization parameters at the **Server**, are specified automatically from the `install.cfg` configuration file.

  To use this file, place it in any of the folders at the first nesting level on the SD card. If the file is downloaded to the device, fields for entering the connection settings will be filled in automatically.

  4. Tap **Connect**.

- **Stations under OS X**

  1. In **Dr.Web Anti-virus** application menu, click **Preferences** and select **Mode**.
  2. Set the **Enable central protection mode** flag.
  3. Parameters of connection to the **Server**, such as IP address and authorization parameters at the **Server**, are specified automatically from the `install.cfg` configuration file.

  To use this file:

  a) Click **Other activation types** in the **License Manager**.

  b) Drag the configuration file to the opened window or click the dotted area to select the file.

  If the file is mounted, fields for entering the connection settings will be specified automatically.

- **Stations under Linux system-based OS**

  1. Open **License Manager** and start the registration procedure by clicking the **Activate license** button.
  2. Select the **Other activation types** option.
  3. In the displayed entry field, specify the path to the configuration file with parameters of configuration and authorization on the **Server**.

2.3.2.2. Installing Dr.Web Agent via the Installer

Agent installer differs from the installation package that it does not contain parameters for connecting to the **Server** and for authorization of the station at the **Server**.

Dr.Web Agent installers are available on the installation page of **Dr.Web Security Control Center**.

To have installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of **Dr.Web Server** first.

Local Installation on Stations under Android OS, Linux OS, OS X

Under Android OS, Linux OS, OS X, installers for **Dr.Web Agent** installation similar to the stand-alone version are available.

Local installation of **Dr.Web Agent** on workstations is described in the **User Manual** for corresponding OS.

If you perform the installation via the installer without the configuration file, you must specify the **Server** address to connect on station manually.

You can either specify authorization parameters manually or leave them blank. At this, the following variants of connection to the **Server** are available:

Setup option	Authorization parameters
Specified manually	Attempt of automatic authorization according to the specified parameters is performed.
Not specified	Authorization mode on the **Server** depends on the **Server** settings for connecting new stations (for more details, see the **Administration Manual**, p. New Stations Approval Policy).

To specify authorization parameters manually, you must create a new station account in the **Control Center** first. At this, the installation package become available, which contains configuration file with connection and authorization parameters. It is recommended to use installation package instead of the installer.

Local Installation on Stations under Windows OS

The following types of **Dr.Web Agent** installers are provided:

- `drwinst.exe` *Network installer* performs the installation of the **Agent** only. After connecting ti the **Server**, the **Agent** downloads and installs necessary anti-virus package components.
- `drweb-esuite-agent-full-10.00.0-`*<build_version>*`-windows.exe` *Full Installer* performs the installation of the **Agent** and anti-virus package at a time.

If you use these installers, you can either specify parameters of authorization and connection to the **Server** manually or leave them blank.

To specify authorization parameters manually, you must create a new station account in the **Control Center** first. At this, the installation package become available. If there is no need to install via the full distribution kit or via network installer, it is recommended to use installation package instead of the installer.

The following variants of connection to the **Server** are available:

Setup option	Server address	Authorization parameters
Specified manually	The station addresses to the specified **Server** directly.	Attempt of automatic authorization according to the specified parameters is performed.
Not specified	**Agent** searches for the **Server** in the network based on the *Server detection service*. Attempt to connect to the first found **Server** is performed.	Authorization mode on the **Server** depends on the **Server** settings for connecting new stations (for more details, see the **Administration Manual**, p. New Stations Approval Policy).

The **User Manual** for Windows OS describes **Dr.Web Agent** installation via the full installer and via the installation package.

It is recommended to perform the installation via the network installer by the anti-virus network administrator.

Local Installation via the Network Installer under Windows OS

The `drwinst.exe` **Agent** network installer is provided to install the **Agent** under Windows OS only.

If the network installer is run in the normal installation mode (i.e. without the `/instMode remove` switch) on stations where the installation has already been performed, this will not incur any actions. The installer program terminates with a help window, contains available switches.

There are two modes of installation via the Network installer:

1. *Background mode* - runs if the background mode switch is specified.
2. *Graphical mode* - default mode. Runs if the background mode switch is not specified.

With the network installer, you can also install **Dr.Web Agent** on a workstation remotely via **Dr.Web Security Control Center** (see p. Remote Installation of Dr.Web Agent).

To install Dr.Web Agent on a workstation in the background mode of the installer:

1. From the workstation, on which you want to install the anti-virus software, enter the network folder of the **Agent** installation (by default at the **Server** installation, it is the `Installer` folder of the **Server** installation folder, further it can be changed) or download from the installation page of the **Control Center** the `drwinst.exe` executable file and `drwcsd.pub` public encryption key. Run the `drwinst.exe` file with the `/silent yes` background mode switch.

   By default, if the `drwinst.exe` file launched without **Server** connection parameters, it will use the **Multicast** mode to scan the network for **Dr.Web Servers** and will try to install **Agent** from the first found **Server**.

When you use the **Multicast** mode to find active **Servers**, the **Agent** installation is performed from the first found **Server**. If the public encryption key is not fit to the **Server** encryption key, installation will be failed. In this case, expressly specify the **Server** address (as described below).

The `drwinst.exe` file also may be used with the optional command line switches:

- If the **Multicast** mode is not used, it is recommended to specify a domain name for **Dr.Web Server** directly (it must be registered on the DNS service):

```
drwinst /silent yes /server <Server_DNS_name>
```

It makes the configuration of the anti-virus network more easy especially in case you reinstall **Dr.Web Server** on a different computer.

- You can expressly specify the **Server** address as follows:

```
drwinst /silent yes /server 192.168.1.3
```

- Using the `/regagent yes` switch during the installation will allow you to register the **Agent** in the **Add or Remove Programs** list.

The complete list of **Network Installer** parameters is describe in the **Appendices** document, p. H2. Network Installer.

2. After the installation is completed, the software of the **Agent** is installed on a computer (anti-virus package is not installed yet).
3. After the station has been approved at the **Server** (if it is required by the **Server** settings), the anti-virus package will be automatically installed.
4. Restart the computer on **Agent** request.

To install Dr.Web Agent on a workstation in the graphical mode of the installer:

From the workstation, on which you want to install the anti-virus software, enter the network folder of the **Agent** installation (by default at the **Server** installation, it is the `Installer` folder of the **Server** installation folder, further it can be changed) or download from the installation page of the **Control Center** the `drwinst.exe` executable file and `drwcsd.pub` public encryption key. Run the `drwinst.exe` file.

A window of the Installation wizard of **Dr.Web Agent** will be opened. Further actions on the **Agent** installation on the stations via the graphical mode of the network installer are similar to the actions on the installation via the installation package, but without **Server** connection settings, if they have not been specified in the corresponding command line switch.

Installation of the **Agent** on workstations is described in the **Dr.Web® Agent for Windows. User Manual**.

2.3.3. Remote Installation of Dr.Web Agent under Windows® OS

Dr.Web Enterprise Security Suite anti-virus allows to detect the computers which are not yet protected by **Dr.Web Enterprise Security Suite**, and in certain cases to install such protection remotely.

Remote installation is available in the following two variants:

- Via the Control Center.
- Via the Active Directory service, if the service is used in the LAN.

Remote installation of **Dr.Web Agents** is possible only on workstations operated by Windows OS (see the **Appendix** document, p. Appendix A. The Complete List of Supported OS Versions) except Starter and Home editions.

Remote installation of **Dr.Web Agents** is possible only from the **Control Center** opened under Windows OS (see the **Appendix** document, p. Appendix A. The Complete List of Supported OS Versions).

To install the anti-virus software on workstations, you must have administrator rights on the correspondent computers.

For remote installation via the **Control Center**, if the workstations are inside a domain and the domain administrative account is used for the installation, you must turn on file and printer sharing on workstations (how to find this option for different Windows OS versions, see in the table below).

If the remote stations are outside a domain, or if the local account is used during the installation, then for some of Windows OS, the extra configuration of the remote stations is required.

Extra Configuration for Remote Installation to a Station outside a Domain or Using the Local Account

Specified options can reduce remote station security. It is strongly recommended to examine functions of these options before editing the system settings or do not use remote installation and install the Agent manually.

After you configure remote workstation, it is recommended to return all changed settings into values before editing to not violate the basic policy of operating system security.

To install the **Agent** to a remote workstation outside a domain, or/and using the local account, do the following on the computer where you want to install the **Agent**:

Operating System	Configuration	
Windows XP	Setup the mode of access to shared files	Modern view: **Start → Settings → Control Panel → Appearance and Themes → Folder Properties →** the **View** tab → clear the **Use Simple Sharing (recommended)** flag
		Classical view: **Start → Settings → Control Panel → Folder Properties →** the **View** tab → clear the **Use Simple Sharing (recommended)** flag
	Set the mode of network authentication model in the local policies	Modern view: **Start → Settings → Control Panel → Performance and Maintenance → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view:

Operating System	Configuration	
		Start → Settings → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves.
	Disable the Windows Firewall on the station before remote installation.	
Windows Server 2003	Disable the Windows Firewall on the station before remote installation.	
Windows Vista Windows Server 2008	Enable the File sharing option	Modern view: **Start → Settings → Control Panel → Network and Internet → Network and Sharing Center → Sharing and discovery → File Sharing → Enable**.
		Classical view: **Start → Settings → Control Panel → Network and Sharing Center → Sharing and discovery → File Sharing → Enable**.
	Set the mode of network authentication model in the local policies	Modern view: **Start → Settings → Control Panel → System and Maintenance → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view: **Start → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	
Windows 7 Windows Server 2008 R2	Turn on file and printer sharing	Modern view: **Start → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**
		Classical view: **Start → Control Panel → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**

Operating System	Configuration	
	Set the mode of network authentication model in the local policies	Modern view: **Start → Control Panel → System and Security → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view: **Start → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	
Windows 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2	Turn on file and printer sharing	Modern view: **Settings → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**
		Classical view: **Settings → Control Panel → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**
	Set the mode of network authentication model in the local policies	Modern view: **Settings → Control Panel → System and Security → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view: **Settings → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER.	

Operating System	Configuration
	b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.

If user account at the remote computer has the empty password, set the access policy with empty password in local policies: **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Accounts: Limit local account use of blank passwords to console logon only** → **Disabled**.

It is necessary to share the location of the **Agent** Installer file `drwinst.exe` and the public encryption key `drwcsd.pub` on the network.

2.3.3.1. Installing Dr.Web Agent Software via Dr.Web Security Control Center

The following means of remote Agent installation on network workstations are available:

1. Installation via the Network Scanner.

   Allows to perform preliminary search of unprotected computers in the network and installation **Dr.Web Agents** on them.

2. Installation using the Network Installation tool.

   Fits for cases, when address of station or groups of stations on which the **Agent** will be installed, is previously known.

3. Installation on stations with specified ID.

   Allows to install **Agents** for selected accounts (including all new accounts) with specified ID and password for **Server** access on stations and groups of stations.

For proper operation of **Network Scanner** and the **Network Installation** tool under Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed **Dr.Web Server** must be added to the trusted sites of browser, on which you open **Control Center** for remote installation.

Using the Network Scanner

In **Dr.Web Security Control Center**, the anti-virus network hierarchical list displays only those computers which are already included into the anti-virus network. The program allows also to discover computers which are not protected with **Dr.Web Enterprise Security Suite** and to install anti-virus components remotely.

To quickly install the **Agent** software on workstations, it is recommended to use **Network Scanner** (see **Administrator Manual**, p. Network Scanner) which searches for computers by IP addresses.

To install Dr.Web Agent via the Network Scanner:

1. Open the **Network Scanner**. On the **Administration** menu of **Dr.Web Security Control Center**, select **Network scanner**. A **Network scanner** window with no data loaded will be opened.

2. Set the **Search by IP addresses**, flag to search for stations in networks by specified IP addresses. In the **Networks** field specify networks in the following format:
   - with a hyphen (for example, `10.4.0.1-10.4.0.10`)
   - separated by a comma with a whitespace (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`)
   - with a network prefix (for example, `10.4.0.0/24`).
3. For Windows OS: set the **Search in Active Directory** flag to search for stations in the Active Directory domain. Specify the following parameters:
   - **Domains** - domains list in which stations are searched. Use comma to divide several domains.
   - **Active Directory controller** - Active Directory controller, e.g., dc.example.com.

To be able to search stations in the Active Directory domain via the **Network Scanner**, the web browser in which the **Control Center** is opened, must be launched in the name of the domain user with permissions to search objects in the Active Directory domain.

Detailed description of additional parameters is given in **Administrator Manual**, the Network Scanner section.

4. Click **Start Scanner**. The catalog (hierarchical list) of computers demonstrating where **Dr.Web Enterprise Security Suite** anti-virus software is installed will be loaded into this window.
5. Unfold the catalog elements corresponding to workgroups (domains). All elements of the catalog corresponding to workgroups and individual stations are marked with different icons the meaning of which is given below.

Table 2-1. Icons of the Network scanner

Icon	Meaning
Workgroups	
	The work groups containing inter alia computers on which **Dr.Web Enterprise Security Suite** anti-virus software can be installed.
	Other groups containing protected or unavailable by network computers.
Workstations	
	The detected station is registered in the DB and active (i.e. the workstation with installed anti-virus software).
	The detected station is registered in the DB as deleted (i.e. the workstation is listed in the table of deleted stations).
	The detected station is not registered in the DB (i.e. there is no anti-virus software on the station).
	The detected station is not registered in the DB (the station is connected to another **Server**).
	The detected station is registered in the DB, bus it is not active and the port is closed.

You can also unfold catalog items corresponding to computers with the or icon, and check which program components are installed there.

6. In the **Network scanner** window, select an unprotected computer (or several unprotected computers by pressing CTRL or SHIFT buttons).
7. On the toolbar, click **Install Dr.Web Agent**.
8. The **Network Installation** window will be opened to configure the **Agent** remote installation task.
9. In the **Computers names** field, specify IP addresses or DNS names of computers on which **Dr.Web Agent** will be installed. If you set several stations, use the space symbol as a separator.

   For installation on stations found via the **Network Scanner**, the address of station or several stations on which installation will be performed already specified in the **Computers names** field.

To install the **Agent** software on several computers at the same time, you can specify several IP addresses in the following format:

- with a hyphen (for example, `10.4.0.1-10.4.0.10`),
- separated by a comma with a whitespace (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
- with a network prefix (for example, `10.4.0.0/24`).

10. By default the **Agent** software is installed to the `%ProgramFiles%\DrWeb` folder. If necessary, specify another location in the **Installation folder** field.

    It is recommended to specify the full path for unique identification of installation folder location. It is allowed to use environment variables in the path.

11. By default the **Server** field displays IP address or DNS name of **Dr.Web Server** to which **Dr.Web Security Control Center** is connected. If necessary, specify the **Server** address from which the anti-virus software will be installed. If you set several **Dr.Web Servers**, use "**;**" or "**;** " as a separator. Leave this field blank to use **Dr.Web Server** detecting service.
12. In the **Public key** field, specify the path to the public encryption key of **Dr.Web Server**.
13. In the **Installer executable file** field, specify the path to the **Network Installer** of **Dr.Web Agent**.

    If public encryption key and **Network Installer** executable file are located in the shared resource, the paths must be specified in the network address format.

14. In the **Language** drop-down list, select the language of interface for **Dr.Web Anti-virus** which will be installed on stations.
15. If necessary, set the **Network installer** command line switches in the **Additional parameters** field (read more in the **Appendices** document, H2. Network Installer).
16. In the **Installation timeout (sec.)** field, specify maximum time to wait for the **Agent** installation to complete in seconds. Valid values: 1-600. 180 seconds is set by default. If network channel capacity between the **Server** and the **Agent** is low, it is recommended to enlarge the value of this option.
17. If necessary, set the **Register installation in Add/Remove Programs list** flag.
18. In the **Install** section, select the components of anti-virus package which will be installed on stations.
19. In the **Compression** and **Encryption** sections, specify the parameters of traffic compression and encryption used by the **Network Installer** during installation of the **Agent** and anti-virus package. These settings also will be used by the **Agent** for interaction with the **Server** after the installation.
20. In the **Authorization on remote PC** section, specify the parameters of authorization to access the remote computers on which the **Agent** will be installed.

    You can set several administrator accounts. To add one more account, click and specify authorization parameters fields. Similarly, for each new record.

    During **Agent** installation, the first account in the list is used at first. If installation under this account failed, the next account in the list is used, and etc.

21. After all necessary parameters have been specified, click **Install**.

    For launching the installation of the anti-virus software, the build-in service is used.

22. **Dr.Web Agent** will be installed on the selected workstations. After the workstation has been approved at the **Server** (if it is required by **Dr.Web Server** settings, see also **Administrator Manual** New Stations Approval Policy), the anti-virus package will be automatically installed.

23. Restart the computer on **Agent** request.

Using the Network Installation Tool

In case an anti-virus network is basically created and it is necessary to install the **Agent** software on certain computers, it is recommended to use ***installation via network***:

1. Select the **Administration** item in the main menu. Then, in the opened window select the **Network installation** item in the control menu.
2. Further steps are similar to **8-22** above.

Installation for Accounts with Specified ID

To perform remote Agent installation for accounts with selected ID:

a) When creating a new station account:

1. Add a new station account or several station accounts (see Creation of a New User Account).
2. Right after adding account, in the right part of a main window, the **Install Dr.Web Agent** pain opens. Click **OK**.
3. The **Network Scanner** window opens.
4. Further steps are similar to **2-23** above.
5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

b) When using existing station account:

1. In the hierarchical list of anti-virus network, select a new station or group of stations, for which **Agents** are not installed, or the **New** group (for installation on all new accounts).
2. Click **Install Dr.Web Agent** on the toolbar.
3. The **Network Scanner** window opens.
4. Further steps are similar to **2-23** above.
5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

Agent installation on stations with selected ID is also available of group administrators.

See the **Appendices** document, the Remote Installation Trouble Shooting section, if an error has occurred.

2.3.3.2. Installing Dr.Web Agent Software via Active Directory

If the **Active Directory** service is used in the LAN, you can remotely install the anti-virus **Agent** on workstations using this service.

The **Agent** installation via Active Directory service is also available when using Distributed File System (see the **Appendices manual**, p. Using DFS During Installation the Agent via the Active Directory section).

Dr.Web Agent Installation

To install the Agent using the Active Directory:

1. Download a copy of **Dr.Web Agent** installer for networks with **Active Directory** at http://download.drweb.com/esuite/.
2. Install **Dr.Web Agent** on the local network server supporting the **Active Directory** service. This can be made in the command line mode **(A)** or in the graphic mode of the installer **(B)**.

If you upgrade the **Server**, you do not have to upgrade **Dr.Web Agent** installer for networks with Active Directory. After upgrading the **Server** software, the **Agents** and the anti-virus software will be upgraded at the stations automatically.

(A) To Set All Necessary Installation Parameters in the Command Line Mode

Issue the following command with all necessary parameters and the obligatory parameter `/qn` which disables the graphic mode:

`msiexec /a <package_name>.msi /qn [<parameters>]`

The `/a` parameter launches installation of the administrative package.

Package name

The name of the installation package for the **Agent** through Active Directory usually has the following format:

`drweb-esuite-agent-activedirectory-<version>-<release_date>.msi`

Parameters:

`/qn` – disable the graphic mode. With this switch the following parameters are to be specified:

- `ESSERVERADDRESS=<DNS_name>` - set the address of **Dr.Web Server** to which the **Agent** is to be connected. For the possible formats see the **Appendices** document, p. Appendix E3.
- `ESSERVERPATH=<path_filename>` - specify the full path to the public encryption key of the **Server** and the file name (by default `drwcsd.pub` in the `Installer` subfolder of the **Server** installation folder).
- `TARGETDIR` – the network folder for the **Agent** image (modified installation package), which will be select via the Group Policy Object Editor for the selected installation. This folder must have read and write access. The path should be given in the network addresses format even if the folder is a locally accessible resource; the folder should be accessible from the target stations.

Before administrative installation, in the destination directory for the **Agent** image (see the `TARGETDIR` parameter), you should not place installation files manually. The **Agent** Installer for networks with Active Directory (`<package_name>.msi`) and other files required for installation of the **Agents** on workstations, will be placed into the destination folder automatically during administrative installation. If these files are present in the destination folder before the administration installation, e.g., from the previous installations, when the similar files will be rewritten.

If you need to perform administrative installation from the different **Servers**, it is recommended to specify different destination folders for each **Server**.

After deployment the administrative package, in the `<destination_dir>\Program Files\DrWeb` directory only the `README.txt` file must resides.

Examples:

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\\win_serv
\drwcs_inst\drwcsd.pub TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:\Program
Files\DrWeb Server\Installer\drwcsd.pub" TARGETDIR=\\comp\share
```

These parameters can alternatively be set in the graphic mode of the installer.

Next on a local network server, where Active Directory administrative tools are installed, appoint installation of the package (see procedure below).

(B) To Set All Necessary Installation Parameters in the Graphic Mode

Before administrative installation, make sure that the destination directory for the **Agent** image does not contain **Dr.Web Agent** Installer for networks with **Active Directory** (*<package_name>*.msi).

After deployment the administrative package, in the *<destination_dir>*\Program Files\DrWeb Enterprise Suite directory only the README.txt file must resides.

1. Issue the command

   msiexec /a *<path>**<package_name>*.msi

2. An **InstallShield Wizard** window with information on the program selected for installation will be opened. Click **Next**.

The **Agent** Installer uses the language specified in the language settings of the computer

3. In the next window, specify the DNS name (preferred form) or the IP address of **Dr.Web Server** (see the **Appendices** document, p. Appendix E3). Specify the location of the public key file of the **Server** (drwcsd.pub). Click **Next**.
4. In the next window type the name of a network catalog, to which the image of the **Agent** is planned to be written. The path should be specified in the network addresses format even if the catalog is a locally accessible resource; the catalog should be accessible from the target stations. Click **Install**.
5. After installation is finished, the settings window displays which helps you configure installation of the package on network workstations.

Installation of the Package on Selected Workstations

1. In **Control Panel** (or in the **Start** menu for Windows 2003/2008 Server OS, in the **Start** → **Programs** menu for the Windows 2000 Server OS), select **Administrative Tools** → **Active Directory Users and Computers** (when you install **Agent** in the graphic mode, this window displays automatically).
2. In the domain containing the computers on which **Dr.Web Agents** are to be installed, create an organizational unit (hereinafter OU), name it, for example, **ESS**. To do this, in the domain context menu, select **New** → **Organizational unit**. In the opened window, type the new unit name and click **OK**. Include the computers, on which the **Agent** is to be installed, into this unit.
3. Open the group policy editor. To do this:

a) for Windows 2000/2003 Server OS: on the OU context menu, select **Properties**. In the opened window go to the **Group Policy** tab.

b) for Windows 2008 Server OS: select **Start** → **Administrative tools** → **Group Policy management.**

4. For the created OU, set the group policy. To do this:
   a) for Windows 2000/2003 Server OS: click **Add** and create an element named **ESS** policy. Double-click it.
   b) for Windows 2008 Server OS: on the OU context menu, select **Create a GPO in this domain, and Link it here**. In the opened window, specify the name of the new group policy object and click **OK**. In the new group policy context menu, select **Edit**.
5. In the **Group Policy Object Editor** window, specify the settings for the group policy created on step 4. To do this:
   a) for Windows 2000/2003 Server OS: in the hierarchical tree, select **Computer Configuration** → **Software Settings** → **Software Installations**.
   b) for Windows 2008 Server OS: in the hierarchical tree, select **Computer Configuration** → **Policies** → **Software Settings** → **Software Installations**.
6. On the context menu of **Software Installations**, select **New** → **Package**.
7. Specify the **Agent** installation package. To do this, specify the address of the network shared resource which contains the **Agent** image you created during the administrative installation. The path should be specified in the network addresses format even if the catalog is a locally accessible resource). Click **OK**.
8. A **Deploy Software** window will be opened. Select the **Assigned** option. Click **OK**.
9. In the **Group Policy Object Editor** window, select the added package. On the context menu of this element, select **Properties**.
10. In the opened package properties window, select the **Deployment** tab. Click the **Advanced** button.
11. An **Advanced Deployment Options** window will be opened.
    - Set the **Ignore language when deploying this package** flag.
    - If you plan to install **Dr.Web Agent** via the customize msi package on 64-bit OS, set the **Make this 32-bit x86 application available to Win64 machines** flag.
12. Click **OK** twice.
13. **Dr.Web Agent** will be installed on selected computers at their next registration in the domain.

Policies Assignment in Consideration of Previous Agent Installations

When you assign an Active Directory policy to install the **Agent**, you should consider a possibility, that the **Agent** is already installed at the station. There are three possible options:

1. **Dr.Web Agent is not installed at the station**.

   After policies assignment, the **Agent** will be installed by general rules.

2. **Dr.Web Agent is already installed at the station without using the Active Directory service**.

   After Active Directory policy assignment, installed **Agent** will remain at the station.

In this case, the **Agent** is installed at the station, but for the Active Directory service **Agent** is not installed. So, after every station startup, attempt of unsuccessful **Agent** installation will be repeated.

To install the **Agent** via the Active Directory, you must uninstall the **Agent** manually (or via the **Control Center**) and assign the Active Directory policy for this station repeatedly.

3. **Dr.Web Agent is already installed at the station via the Active Directory**.

   Repeated assignment of a policy to a stations with **Dr.Web Agent** installed via the Active Directory service is not performed.

   Thus, policies assignment will not take any affect to the anti-virus software state at the station.

2.4. Installing NAP Validator

Dr.Web NAP Validator checks health of anti-virus software on protected workstations. It is installed on the computer where a configured NAP server resides.

To install NAP Validator

1. Run the installation file. In the dialog window, select the language to use during install. Select **English** and click **Next**.
2. On the Welcome page of the **InstallShield Wizard**, click **Next**.
3. On the **License Agreement** page, read the agreement. To accept the agreement and proceed with the installation, select **I accept the terms of the license agreement** and click **Next**. To exit the wizard, click **Cancel**.
4. On the next page, specify **Dr.Web Server** IP **Address** and **Port** and click **Next**.
5. Click **Install**. The installation begins.
6. When installation completes, click **Finish**.

After you install **Dr.Web NAP Validator**, add **Dr.Web Server** to the trusted NAP servers group.

To add Dr.Web Server to the trusted NAP servers group

1. To open NAP server configuration component, run the `nps.msc` command.
2. In the **Remediation Servers Group** section, click **Add**.
3. In the dialog window, enter the name for the new remedial server and **Dr.Web Server** IP address.
4. Click **OK** to save changes.

2.5. Installing Proxy Server

One or several **Proxy servers** can be included into the anti-virus network.

When choosing a computer where the **Proxy server** should be installed, consider that it should be accessible from all networks and segments which require data redirection between them.

To install the **Proxy server**, you must have administrator rights on this computer.

To establish a connection between the **Server** and clients via the **Proxy server**, it is recommended to disable traffic encryption. For this, it is enough to set the **no** value for the **Encryption** parameter in the **Dr.Web Server Configuration** section (see the **Administrator Manual**, p. Dr.Web Server Configuration > General).

Below is described the installation of the **Proxy server** for Windows OS. The set and the order of steps may somewhat differ depending on the distribution file version.

To install the Proxy Server on a computer operated by Windows OS

1. Run the distribution file. A window of **Installation Wizard** with information about the program to be installed will be opened. Click **Next**.

2. A window with the text of the license agreement will be opened. You should read and accept the agreement. To continue the installation, in the bottom part of the window select **I accept the terms of the license agreement** and click **Next**.
3. A window for setting general **Proxy server** parameters will be opened:
   - In the **Listen to** field, specify the IP address, which will be "listened" by the **Proxy server**. By default, it is `any (0.0.0.0)` value, which means "listen" for all interfaces.

Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

   - In the **Port** field, specify a port, which will be listened by the **Proxy server**. By default, it is the **2193** port.
   - In the **Protocol** drop-down list, select a type of the protocol for accepting incoming connections by the **Proxy server**.
   - Set the **Enable discovery** flag to enable the **Server** imitation mode. This mode allows **Network scanner** to detect the **Proxy server** as **Dr.Web Server**. For the the **Server** imitation mode, the following settings are available:
     - Set the **Enable multicasting** flag so the **Proxy server** will reply to a multicast requests addressed to the **Server**.
     - In the **Multicast group**, specify an IP address of a multicast group, in which the **Proxy server** is included. Specified interface will be listened by the **Proxy server** for interaction with **Network installers** during active **Dr.Web Servers** searching. If you leave this field blank, **Proxy server** will not be included in any of multicast groups. Default multicast group to which the **Server** is included is `231.0.0.1`.
   - In the **Compression mode** drop-down list, select the compression mode of traffic for channels between **Proxy server** and served clients: **Agents** and **Agent** installers. In the **Level** field, specify the compression level. Integers from 1 to 8 are allowed.

   After you specified general settings, click **Next**.

4. A window for setting cache parameters of the **Proxy server** will be opened:

   Set the **Enable caching** flag to cache the data transferred by the **Proxy server** and specify the following parameters:

   - To change the default folder for storing cached data, click **Browse** and specify a new folder in the file system browser.
   - In the **Maximum revisions number** field, specify the maximal number of stored revisions. By default, 3 last revisions are stored, the older revisions are deleted.
   - In the **Cleanup interval** field, specify the time interval in minutes between deletions of old revisions. Default is 60 minutes.
   - In the **Unload interval** field, specify the time interval in minutes between unloads of unused files from the memory. Default is 10 minutes.
   - In the **Integrity check mode** drop-down list, select the check mode of cache integrity:
     - **At startup** - at a startup of the **Proxy server** (may take a long time).
     - **Idle** - in the background of the **Proxy server** operating.

   After you specified cache settings, click **Next**.

5. A window for configuring connections redirection will be opened:

   In the **Redirection settings** section, specify an address or the list of addresses of **Dr.Web Servers**, to which the connections established by the **Proxy server** will be redirected.

Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

In the **Compression mode** drop-down lists, select the compression mode of traffic for channels between **Proxy server** and each of the specified **Dr.Web Servers**.

After you specify redirection settings, click **Next**.

6. A window for changing the installation folder will be opened. If you want to change the default folder, click **Change** and specify the installation folder. Click **Next**.
7. A window with information, that the **Proxy server** is ready to install, will be opened. Click **Install** to begin the installation process.
8. Once the installation is complete, click **Finish**.

After installation, if necessary, you can change operation parameters of the **Proxy server**. For this use the `drwcsd-proxy.xml` configuration file which is located in the **Proxy server** installation folder. Parameters of the configuration file are given in the **Appendices** document, p. Appendix G4.

Package-based installation of the Proxy Server on a UNIX system-based OS

Use the following command:

- for **FreeBSD** OS:

  `pkg_add` *<distribution_file_name.tbz>*
- for **Solaris** OS:

  `bzip2 -d` *<distribution_file_name.bz2>* and then:

  `pkgadd -d` *<distribution_file_name>*
- for **Linux** OS:
- for **Debian** OS and **Ubuntu** OS:

  `dpkg -i` *<distribution_file_name.deb>*
- for **rpm distribution kits**:

  `rpm -i` *<distribution_file_name.rpm>*

Also, there are so-called `generic` packages, which can be installed on any Linux-based system including those which are not on the list of supported systems. They are installed by means of the installer included in the package:

`tar -xjf` *<distribution_file_name.tar.bz2>*

After that you need to move all unpacked folders into the root directory.

In the course of the installation for **FreeBSD** OS an `rc` script `/usr/local/etc/rc.d/0.dwcp-proxy.sh` will be created.

- To manually stop the **Proxy server**, use the command:
  `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop`
- To manually start the **Proxy server**, use the command:
  `/usr/local/etc/rc.d/0.dwcp-proxy.sh start`

During the installation for **Linux** OS and **Solaris** OS, an `init` script `(/etc/init.d/dwcp-proxy)` for the launching and termination of the **Server** will be created.

Chapter 3: Removal of Dr.Web Enterprise Security Suite Components

3.1. Removing Dr.Web Server

3.1.1. Removing Dr.Web Server for Windows® OS

To remove **Dr.Web Server** (general and extra distribution kits) or **Dr.Web Security Control Center Extension** software, run the installation file of the corresponding product of currently installed version. The installation program will automatically detect the software product and offer to remove it. To remove software, click **Remove**.

Dr.Web Server (general and extra distribution kits) and **Dr.Web Security Control Center Extension** software can also be removed using standard Windows OS tools via the **Control Panel** → **Add or Remove Programs**.

When removing the **Server**, configuration files, encryption keys and embedded database are back up only if you set the **Back up Dr.Web Server critical data** option.

3.1.2. Removing Dr.Web Server for UNIX® System-Based OS

Deinstallation should be carried out under the superuser account (**root**).

Removing general distribution kit of Dr.Web Server

1. Server deinstallation procedure depends on operating system and **Server** version installed.

a) To deinstall the **Server** of **6.XX** version and earlier, perform the following actions:

Server OS		Action
FreeBSD		Execute the command: `pkg_delete drweb-esuite`
Solaris		1. Stop the **Server**: `/etc/init.d/drwcsd stop` 2. Execute the command: `pkgrm DWEBesuit`
Linux	Debian Ubuntu	Execute the command: `dpkg -r drweb-esuite`
	rpm package	Execute the command: `rpm -e drweb-esuite`
	generic package	Run the script: `/opt/drwcs/bin/drweb-esuite-uninstall.sh`

b) To deinstall the **Server** of **10.0** version, perform the following actions:

Server OS	Action
FreeBSD	Run the script: `/usr/local/etc/opt/software/drweb-esuite.remove`

Server OS		Action
Solaris		1. Stop the **Server**: `/etc/init.d/drwcsd stop` 2. Execute the command: `drweb-esuite`
Linux	Debian Ubuntu	Execute the command: `dpkg -P drweb-esuite`
	rpm package	Execute the command: `rpm -e drweb-esuite`
	generic package	Run the script: `/etc/opt/drweb.com/software/drweb-esuite.remove`

2. On **Solaris** OS, you will be asked to confirm that you really want to uninstall the software and agree to run the deinstallation scripts on behalf of the administrator (**root**).

At removing the **Server** under **FreeBSD** OS and **Linux** OS, the **Server** operations will be immediately terminated, the database, key and configuration files will be copied to `/var/tmp/drwcs` default backup folder.

Removing extra distribution kit of Dr.Web Server

1. To deinstall the extra distribution kit of the **Server** of **10.0** version, perform the following actions:

Server OS		Action
FreeBSD		Run the script: `/usr/local/etc/opt/software/drweb-esuite-extra.remove`
Solaris		1. Stop the **Server**: `/etc/init.d/drwcsd stop` 2. Execute the command: `drweb-esuite-extra`
Linux	Debian Ubuntu	Execute the command: `dpkg -P drweb-esuite-extra`
	rpm package	Execute the command: `rpm -e drweb-esuite-extra`
	generic package	Run the script: `/etc/opt/drweb.com/software/drweb-esuite-extra.remove`

2. On **Solaris** OS, you will be asked to confirm that you really want to uninstall the software and agree to run the deinstallation scripts on behalf of the administrator (**root**).

Removing Dr.Web Security Control Center Extension

To remove **Dr.Web Security Control Center Extension**, execute the following command:

Package type	Command
deb-package	`dpkg -P drweb-esuite-plugins`
rpm-package	`rpm -e drweb-esuite-plugins`

other packages (**tar.bz2** and **tar.gz**)	`rm -f <plugins_directory>/libnp*.so`
	For exmaple, for Mozilla Firefox browser:
	`rm -f /usr/lib/mozilla/plugins/libnp*.so`

3.2. Removing Dr.Web Agent

Removing of **Dr.Web Agent** from protected stations can be performs by the following ways:

- For stations under Windows OS:
  - Remotely via the Control Center.
  - Locally on station.
  - Via the Active Directory service, if the **Agent** was installed using this service.
- For stations under Android OS, Linux OS, OS X - locally on stations.

Removing of **Dr.Web Agent** on workstations under Android OS, Linux OS, OS X is described in the **User Manual** for corresponding OS.

3.2.1. Removing Dr.Web Agent for Windows® OS

Uninstalling Dr.Web Agent and Anti-Virus Package Remotely

Remote installation and removal of the **Agent** software is possible within a local network only and requires administrator's rights in the local network.

If you uninstall the **Agent** and anti-virus package via the **Control Center**, the **Quarantine** will not be deleted from the station.

To uninstall the anti-virus software from a workstation (for Windows OS only):

1. Select the **Anti-virus network** item in the main menu of **Dr.Web Security Control Center**.
2. In the opened window select the necessary group or certain anti-virus stations.
3. Click **General** → **Uninstall Dr.Web Agent** in the toolbar of the anti-virus network catalog.
4. The **Agent** software and the anti-virus package will be removed from the workstations selected.

In case **Agent** removal is instructed when there is no connection between **Dr.Web Server** and the anti-virus workstation, the **Agent** software will be uninstalled from the selected computer once the connection is recovered.

Uninstalling Dr.Web Agent and Anti-Virus Package Locally

To remove the **Agent** and the anti-virus package locally, this option must be allowed at the **Server** in the **Rights** section.

You can remove the station anti-virus software (**Agent** and anti-virus package) by the two ways:

1. By means of standard Windows OS services.
2. By using the Agent installer.

If the **Agent** and anti-virus package are uninstalled via the standard Windows OS services or via the **Agent** installer, user will be prompt for **Quarantine** deleting.

Removing by Means of Standard Windows OS Services

This removing method will be available only if you installed the **Agent** by using the graphical installer and set the **Register Agent in system list of installed software** flag.

If the **Agent** installed in the background mode of the installer, the removing of the anti-virus software with the standard Windows OS services will be available only if the `/regagent yes` switch was used for installation.

To remove the **Agent** and the anti-virus package, use standard Windows OS tools: the **Add or Remove Programs** element in **Control Panel** (see the **Agent User Manual** for details).

Removing by Using the Agent Installer

- **Client module win-es-agent-setup.exe**

  To remove the **Agent** software and the anti-virus package by using the client module which is created during the **Agent** setup, run the `win-es-agent-setup.exe` installation file with the `/instMode remove parameter`. Additionally use the `/silent no` parameter, if you want to control the process.

  The `win-es-agent-setup.exe` installation file is located in the following folder by default:

  - For Windows XP OS and Windows Server 2003 OS:
    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - For Windows Vista OS and later and Windows Server 2008 OS and later:
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  For example, for Windows 7, where the `%ALLUSERPROFILE%` corresponds to `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode remove /silent no
  ```

- **Installation package drweb-esuite-install.exe**

  To remove the **Agent** software and the anti-virus package by using the installation package, run the `drweb-esuite-install.exe` installation file of the currently installed version.

- **Full installer drweb-esuite-agent-full-10.00.0-*<build_version>*-windows.exe**

  To remove the **Agent** software and the anti-virus package by using the full installer, run the `drweb-esuite-agent-full-10.00.0-`*<build_version>*`-windows.exe` installation file of the currently installed version.

- **Network installer drwinst.exe**

  To remove the **Agent** software and the anti-virus package from a workstation locally by using the network installer, run in the installation folder of the **Agent** (by default `C:\Program Files\DrWeb`) the `drwinst.exe` installer with the `/instMode remove` parameter. Additionally use the `/silent no` parameter, if you want to control the process.

For example:

```
drwinst /instMode remove /silent no
```

When you launch the `drweb-esuite-install.exe` installation package, the `drweb-esuite-agent-full-10.00.0-<build_version>-windows.exe` full installer and the `drwinst.exe` network installer, the `win-es-agent-setup.exe` client module launches and performs the removal directly.

The `win-es-agent-setup.exe` client module launched without parameters, detects installed product and launches the change/remove mode. To launch the remove mode directly, use the `/instMode remove` switch.

3.2.2. Removing Dr.Web Agent through Active Directory

1. In **Control Panel**, select **Administrative Tools** → **Active Directory users and computers**.
2. Right-click your **ESS** organizational unit in the domain. On the context menu, select **Properties**. An **ESS Properties** window will be opened.
3. Go to the **Group Policy** tab. Select **ESS policies**. Double-click the item. A **Group Policy Object Editor** window will be opened.
4. In the hierarchical list, select **Computer configuration** → **Software settings** → **Software installations** → **Package**. Then on the context menu, select **All tasks** → **Uninstall** → **OK.**
5. On the **Group Policy** tab, click **OK.**
6. **Dr.Web Agent** will be removed from the stations at the next registration in the domain.

3.3. Removing Proxy Server

Uninstalling Proxy Server for Windows OS

During **Proxy server** uninstallation, the `drwcsd-proxy.xml` configuration file is deleted. If necessary, save configuration file manually before **Proxy server** uninstallation.

The **Proxy server** software uninstallation is performed via the standard Windows OS tools at **Control Panel** → **Add or Remove Programs** (**Programs and components** for Windows 2008 OS).

Uninstalling Proxy Server for UNIX System-Based OS

Proxy server OS		Action
FreeBSD		Run the script: `/usr/local/etc/opt/software/drweb-proxy.remove`
Solaris		Execute the command: `pkgrm drweb-esuite-proxy`
Linux	deb package	Execute the command: `dpkg -P drweb-esuite-proxy`
	rpm package	Execute the command: `rpm -e drweb-esuite-proxy`
	generic package	Run the script: `/etc/opt/drweb.com/software/drweb-proxy.remove`

Chapter 4: Updating Dr.Web Enterprise Security Suite Software and Its Components

Before updating **Dr.Web Enterprise Security Suite** and its components, please note the following important features:

- Before updating, it is recommended to check the validity of TCP/IP protocol configuration for the Internet access. Particularly, DNS service must be enabled and properly configured.
- In multiserver anti-virus network configuration, consider that interserver updates transmission is not performed between **Servers** of **10.0** version and **Servers** of previous versions and interserver connection is used for transmission statistics only. To provide interserver updates transmission, you must upgrade all **Servers**. If you need to remain **Servers** of previous version as a part of the anti-virus network to connect the **Agents** installed on operating systems which are not supported by the **10.0** version (see Upgrading Dr.Web Agent), when **Servers** of **6.XX** versions and **Servers** of the **10.0** version must receive updates independently.
- During upgrade of the **Server** from the **6.XX** version to the **10.0** version, settings of the **Sever** operation via the proxy server are not saved. After the installation of the **10.0** version, you must specify the settings of connection via the proxy server manually (see **Administration Manual**, p. Proxy).
- During automatic upgrade of **Agents**, the old version of **Agent** is deleted and the new version is installed. Installation of a new **Agent** version is performed according to the task from the **Server** schedule, which is executed after reboot of a station. Station reboot must be launched manually after the old version of **Agent** is deleted.

Notification on reboot required is not displayed on a station. Administrator must initiate the station reboot.

Between the removal of an old **Agent** version and installing of a new version, stations will have no anti-virus protection.

4.1. Upgrading Dr.Web Server for Windows® OS

Upgrading of the **Server** from the **6** version to the **10** version and within version **10** is performed automatically by the means of the installer.

Before removing the **Server** of previous version, please read the Upgrading Dr.Web Agent section.

Upgrading the **Server** within version **10** can be also performed via the **Control Center**. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Not all **Server** updates within version **10** have the distribution kit file. Some of them can be installed via the **Control Center** only.

Saving Configuration Files

After the **Server** of **6.X** version has been removed, the following files are automatically saved:

File	Description	Default folder
`agent.key` (name may vary)	**Agent** license key file	`etc`
`certificate.pem`	SSL certificate	
`drwcsd.conf` (name may vary)	**Server** configuration file	
`drwcsd.pri`	private encryption key	
`enterprise.key` (name may vary)	**Server** license key file	
`private-key.pem`	RSA private key	
`auth-ads.xml`	configuration file for administrators external authorization via Active Directory	
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP	
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS	
`dbinternal.dbs`	embedded database	`var`
`drwcsd.pub`	public encryption key	• `Installer` • `webmin\install`

After the **Server** of **10.0** version has been removed, the following files are saved:

File	Description	Default folder
`agent.key` (name may vary)	**Agent** license key file	`etc`
`enterprise.key` (name may vary)	**Server** license key file. The file is saved if it presented after the upgrade from the previous versions. For the new **Server 10.0** installation, the file is absent	
`frontdoor.conf`	configuration file for the **Server** remote diagnostic utility	
`proxy.conf`	proxy server configuration file	
`auth-ads.xml`	configuration file for administrators external authorization via Active Directory	
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP	
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS	
`download.conf`	network settings for generating of the **Agent** installation packages	
`drwcsd.conf` (name may vary)	**Server** configuration file	
`drwcsd.conf.distr`	**Server** configuration file template with default parameters	
`drwcsd.pri`	private encryption key	

File	Description	Default folder
openssl.cnf	Server certificate for HTTPS	
webmin.conf	Dr.Web Security Control Center configuration file	
dbexport.gz	database export	*<backup>* folder
drwcsd.pub	public encryption key	• Installer • webmin\install

If you are planning to use configuration files from the previous version of the **Server**, please note:

1. **Server** license key is no longer supported (see Licensing).
2. The embedded database is upgraded and configuration files of the **Server** is converted by the means of the installer. You cannot replace these files with a backup copies when upgrading to the **Server 10.0**.

If necessary, copy other critical files you want to preserve to another folder, other than **Server** installation folder. For instance, report templates which are stored in the `\var\templates` folder.

Saving Database

The MS SQL CE database starting from the **10.0** version of **Dr.Web Server** is no longer supported. During automatic **Server** upgrade by the means of the installer, the MS SQL CE database is automatically converted to the IntDB embedded database.

Before upgrade **Dr.Web Enterprise Security Suite** software, it is recommender to backup database.

To backup database:

1. Stop the **Server**.
2. Export DB to the file:
   `"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb` *<backup_folder>*`\esbase.es`

For **Servers** with external DB, it is recommended to use standard tools supplied with the database.

Make sure, that **Dr.Web Enterprise Security Suite** DB export completed successfully. If DB backup copy is not available, the **Server** could not be restored in emergency case.

Upgrading Dr.Web Server

To upgrade Dr.Web Server:

1. Run the distribution file.

By default, installer uses the language of the operating system. If necessary, you can change the installation language on any step by selecting the corresponding option in the right upper part of the installer window.

2. The window opens, which notifies you on the previous **Dr.Web Server** version installed and brief description of the upgrade process to a new version. To start configuring upgrade procedure, click **Upgrade**.

3. A window with information on the product and the link to the license agreement text will be opened. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
4. On the following steps of the installation wizard, the upgrading **Server** is configured as at the Installing Dr.Web Server process based on the configuration files from the previous installation (see above). The installation wizard automatically locates the **Server** installation folder, configuration files and embedded DB location from the previous installation. If necessary, you can change locations of the files which were found automatically by the installer.

For the external **Server** database, also select **Use existing database** during upgrade.

If you are going to use the Oracle or PostgreSQL DB as an external database via the ODBC connection, then during upgrading of the **Server**, in the installer settings, disable the installation of embedded client for PostgreSQL DBMS (in the **Database support** section).

Otherwise, interaction with the Oracle DB via ODBC will fail because of the libraries conflict.

5. To remove the **Server** of the previous version and launch the installation process of the **10.0** version of the **Server**, click **Install**.

After upgrade of anti-virus network **Servers** is completed, you must configure encryption and compression settings for the connected **Servers** (see the **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).

After upgrading of Dr.Web Server to 10.0 version perform the following to ensure normal operation of Dr.Web Security Control Center:

1. Clear cache of the Web browser that is used to connect to **Dr.Web Security Control Center**.
2. Upgrade **Dr.Web Security Control Center Extension**.

4.2. Upgrading Dr.Web Server for UNIX® System-Based OS

All actions must be performed under the **root** administrator account.

Upgrading the **Server** software of the previous version to version **10** is possible not for all UNIX system-based OS. Thus, under UNIX system-based OS, in which upgrading is not supported, it is recommended to delete the **Server** software of previous versions saving the backup copy and install the **10.0** version based on the saved backup copy.

Upgrading the **Server** software within version **10** for the same package types is performed automatically.

Before removing the **Server** of previous version, please read the Upgrading Dr.Web Agent section.

Upgrading the **Server** within version **10** can be also performed via the **Control Center**. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Not all **Server** updates within version **10** have the distribution kit file. Some of them can be installed via the **Control Center** only.

Saving Configuration Files

After the **Server** of **6.X** version has been removed, the following files are automatically saved:

File	Description	Default folder
`agent.key` (the name may vary)	**Agent** license key file	• for Linux OS and Solaris OS: /var/opt/drwcs/etc • for FreeBSD OS: /var/drwcs/etc
`certificate.pem`	SSL certificate	
`download.conf`	network settings for generating of the **Agent** installation packages	
`drwcsd.conf` (the name may vary)	**Server** configuration file	
`drwcsd.pri`	private encryption key	
`enterprise.key` (the name may vary)	**Server** license key file	
`private-key.pem`	RSA private key	
`webmin.conf`	**Dr.Web Security Control Center** configuration file	
`common.conf`	configuration file (for some UNIX system-based OS)	
`local.conf`	**Server** log settings	
`dbinternal.dbs`	embedded database	• for Linux OS and Solaris OS: /var/opt/drwcs/ • for FreeBSD OS: /var/drwcs/
`drwcsd.pub`	public encryption key	• for Linux OS and Solaris OS: /opt/drwcs/Installer/ /opt/drwcs/webmin/install • for FreeBSD OS: /usr/local/drwcs/Installer/ /usr/local/drwcs/webmin/install

After the **Server** of **10.0** version has been removed, the following configuration files are automatically saved to the default backup folder:

File	Description	Default folder
`agent.key` (the name may vary)	**Agent** license key file	`/var/tmp/drwcs/`
`certificate.pem`	SSL certificate	
`download.conf`	network settings for generating of the **Agent** installation packages	
`drwcsd.conf` (the name may vary)	**Server** configuration file	

File	Description	Default folder
drwcsd.pri	private encryption key	
enterprise.key (the name may vary)	**Server** license key file. The file is saved if it presented after the upgrade from the previous versions. For the new **Server 10.0** installation, the file is absent	
frontdoor.conf	configuration file for the **Server** remote diagnostic utility	
private-key.pem	RSA private key	
webmin.conf	**Dr.Web Security Control Center** configuration file	
common.conf	configuration file (for some UNIX system-based OS)	
local.conf	**Server** log settings	
dbexport.gz	database export	
drwcsd.pub	public encryption key	

After the automatic upgrade for **Linux** OS and **Solaris** OS, the following files are also saved:

For the **Server 6.X**:

File	Description	Default folder
auth-ldap.xml	configuration file for administrators external authorization via LDAP	/var/opt/drwcs/etc
auth-radius.xml	configuration file for administrators external authorization via RADIUS	

For the **Server 10.0**:

File	Description	Default folder
auth-ldap.xml	configuration file for administrators external authorization via LDAP	/var/tmp/drwcs/
auth-pam.xml	configuration file for administrators external authorization via PAM	
auth-radius.xml	configuration file for administrators external authorization via RADIUS	

If you are planning to use configuration files from the previous version of the **Server**, please note:

1. **Server** license key is no longer supported (see Licensing).
2. The embedded database is upgraded and configuration files of the **Server** is converted by the means of the installer. You cannot replace these files with a backup copies when upgrading to the **Server 10.0**.

Saving Database

Before upgrade **Dr.Web Enterprise Security Suite** software, it is recommender to backup database.

To backup database:

1. Stop the **Server**.
2. Export DB to the file:
   - For FreeBSD OS:
     ```
     # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
     ```

- For Linux OS:
  ```
  # /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
  ```
- For Solaris OS:
  ```
  # /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
  ```

For **Servers** with external DB, it is recommended to use standard tools supplied with the database.

Make sure, that **Dr.Web Enterprise Security Suite** DB export completed successfully. If DB backup copy is not available, the **Server** could not be restored in emergency case.

Automatic Upgrade

If you update the **Server** from **6.0** and later versions to **10.0** version for **Linux** and **Solaris** OS, instead of deleting old version and installing new version of the **Server**, you can use the package update of the **Server**. For this, launch the installation of corresponding **Server** package.

All automatically saved files will be stored in corresponding directories and manual replacement is not required.

Manual Upgrade

If using an embedded database:

1. Stop the **Server**.
2. If you plan to use any files (besides files which are copied automatically during **Server** uninstall at step **4**), backup these files manually. For instance, copy the report templates to a backup folder.
3. Remove all contents of the repository.
4. Remove **Dr.Web Server** software (see Removing Dr.Web Server Software for UNIX® System-Based OS). You will be prompt to create backup copies of files. For this, specify a folder where to store the backup or accept the default folder.
5. Install **Dr.Web Server** version **10.0** according to the general installation procedure (see Installing Dr.Web Server for UNIX® System-Based OS) based on the backup copy from the step **4**. All saved configuration files and embedded database will be automatically converted for the **Server** of the **10.0** version. Without automatic conversion, database and some of **Server** configuration files from the previous version cannot be used.

   In case of manual backup, replace the files in the same folders from which you copied the files before new install.

For all backup files from the previous **Server** version (see step **6**) assign the user, selected at the installation of the new **Server** version (**drwcs** by default), as files owner.

6. Launch the **Server**.
7. Set up repository upgrade and perform the upgrade.
8. Restart the **Server**.

If using an external database:

1. Stop **Dr.Web Server**.
2. If you plan to use any files (besides files which are copied automatically during **Server** uninstall at step **4**), backup these files manually. For instance, copy the report templates to a backup folder.
3. Remove the contents of the repository.
4. Remove **Dr.Web Server** software (see the Removing Dr.Web Server Software for UNIX® System-Based OS section). You will be prompt to create backup copies, for this, specify a folder where to store the backup or accept the default folder.

5. Install **Dr.Web Server** version **10.0** (see p. Installing Dr.Web Server for UNIX® System-Based OS).
6. Move the automatic saved files (see above) to:
   - for **Linux** OS: to `/var/opt/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/` and to `/opt/drwcs/webmin/install`
   - for **FreeBSD** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/usr/local/drwcs/Installer/` and to`/usr/local /drwcs/webmin/install`
   - for **Solaris** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/` and to `/opt/drwcs/webmin/install`

   In case of manual backup, replace the files in the same folders from which you copied the files before new install.

For all backup files from the previous **Server** version (see step **6**) assign the user, selected at the installation of the new **Server** version (**drwcs** by default), as files owner.

7. To upgrade the databases, execute the following commands:
   - for **Linux** OS and **Solaris** OS:
     ```
     /etc/init.d/drwcsd upgradedb
     ```
   - for **FreeBSD** OS:
     ```
     /usr/local/etc/rc.d/drwcsd.sh upgradedb
     ```
8. Launch **Dr.Web Server**.
9. Set up repository upgrade and perform the upgrade.
10. Restart the **Server**.

After upgrade of anti-virus network **Servers** is completed, you must configure encryption and compression settings for the connected **Servers** (see the **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).

4.3. Upgrading Dr.Web Security Control Center Extension

To upgrade **Dr.Web Security Control Center Extension** (is used by **Dr.Web Security Control Center**), delete **Dr.Web Security Control Center Extension** software of current versions and install the new version.

Deletion of the **Dr.Web Security Control Center Extension** is described in the Removing Dr.Web Server for Windows® OS or Removing Dr.Web Server for UNIX® System-Based OS sections.

Installation is described in the Installing Dr.Web Security Control Center Extension section.

4.4. Upgrading Dr.Web Agent

The **Agent** upgrade after the **Server** upgrade is described for the following variants:

1. Upgrading Dr.Web Agents on Stations under Windows® OS,
2. Upgrading Dr.Web Agents on Stations under Linux, Android OS X.

4.4.1. Upgrading Dr.Web Agents on Stations under Windows® OS

Automatic Upgrade

To perform automatic upgrade, the following conditions must be met:

1. **Agents** must be installed on a computers under Windows OS which are supported for the installation of **Agents** for **Dr.Web Enterprise Security Suite** version **10.0** (see the **Appendices** document, Appendix A. The Complete List of Supported OS Versions).
2. For the automatic upgrade, the following actions are possible depending on the **Server** settings:
   a) Automatic upgrade is performed, if during the **Server** upgrade, encryption keys and network settings from the previous **Server** were saved.
   b) The manual configuration required during the automatic upgrade, if during the **Server** upgrade, new encryption keys and **Server** network settings were specified.

Please note the following features during automatic upgrade:

1. After removing the **Agent**, notification on reboot required is not displayed on a station. Administrator must initiate the station reboot.
2. Between the removal of an old **Agent** version and installing of a new version, stations will have no anti-virus protection.
3. After upgrading of the **Agent**, the anti-virus software operation will be limited without the station restart. At this, the complete anti-virus protection of the station is not provided. User must restart the station on the **Agent** demand.

Automatic upgrade of the Agent is performed by the following procedure:

1. The old version of the **Agent** is uninstalled when upgrade is started.
2. The station is rebooted manually.
3. The new version of the **Agent** is installed. For this, the task in the **Server** schedule is automatically created.
4. After the **Agent** upgrade is completed, the station automatically connects to the **Server**. In the **Status** section of the **Control Center**, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Automatic upgrade of the Agent with manual configuring is performed by the following procedure:

1. Configure settings for connection to the new **Server** and replace public encryption key on station manually.
2. After changing of the settings on the station and connecting the stations to the **Server**, the **Agent** upgrade process starts.
3. The old version of the **Agent** is uninstalled when upgrade is started.
4. The station is rebooted manually.
5. The new version of the **Agent** is installed. For this, the task in the **Server** schedule is automatically created.
6. After the **Agent** upgrade is completed, the station automatically connects to the **Server**. In the **Status** section of the **Control Center**, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Manual Upgrade

If installation of the new version of the **Agent** during automatic upgrade failed for any reason, the next installation attempts are not performed. No anti-virus software will be installed on the station, and such station will be displayed as offline in the **Control Center**.

In such case, you must install the Agent by yourself. At this, after the new **Agent** installation, you must merge the new station and the old station in the **Control Center**, in the hierarchical tree of the anti-virus network.

Upgrade is not Supported

If **Agents** are installed on stations under OS which are not supported for the installation of **Agents** for **Dr.Web Enterprise Security Suite** version **10.0**, actions to upgrade are not performed.

Agents installed on unsupported OS cannot receive updates (including virus bases updates) from the new **Server**. If you need to remain **Agents** under unsupported OS, you must leave the **Server** of previous version to which these **Agents** are connected as a part of the anti-virus network. At this, **Servers** of **6.XX** versions and **Servers** of the **10.0** version must receive updates independently.

Recommendations on upgrading the **Agents**, installed at the stations that implement significant LAN functions, specified in the **Appendices** document, p. Upgrading Dr.Web Agents on the LAN servers.

4.4.2. Upgrading Dr.Web Agents on Stations under Linux, Android OS X

Agents installed on stations under Linux system-based OS, Android OS and OS X connect to the **Server** of the **10.0** version with complete support of updating process in the following cases:

1. **Agents** must be installed on a computers under operation systems which are supported for the installation of **Agents** for **Dr.Web Enterprise Security Suite** version **10.0** (see the **Appendices** document, Appendix A. The Complete List of Supported OS Versions).
2. Encryption keys and network settings from the upgraded **Server** must be set on the stations.

4.5. Upgrading Proxy Server

Upgrading Proxy Server for Windows OS

Automatic update of **Proxy server** is not supported.

When you run the installer on a PC with installed **Proxy server**:

- If the installer has the same bit depth as an installed **Proxy server**, notification about impossibility of installation is shown.
- If the bit depth of installer differs from bit depth of installed **Proxy server**, the **Proxy server** is installed in the folder different from the folder of installed version.

Installation of two **Proxy servers** on the same PC and configuring them to operate via the same port leads to inoperability of both **Proxy servers**.

To upgrade Proxy server:

1. If on a computer with installed **Proxy server**, the **Agent** with enabled self-protection is installed, disable **Dr.Web Self-protection** component via the **Agent** settings.
2. Uninstall the **Proxy server** according to the standard procedure (see Removing Proxy Server).

During **Proxy server** uninstallation, the `drwcsd-proxy.xml` configuration file (see the **Application** document, p. Appendix G4) is deleted. If necessary, save configuration file manually before **Proxy server** uninstallation.

3. Install a new version of **Proxy server** according to the standard procedure (see Installing Proxy Server).
4. If necessary, replace configuration file with manually saved one from the previous version.
5. If you disabled **Dr.Web Self-protection** component at step 1, enable it via the **Agent** settings.

Upgrading Proxy Server for UNIX System-Based OS

To upgrade the proxy server:

1. During **Proxy server** upgrading, the `drwcsd-proxy.xml` configuration file (see the **Application** document, p. Appendix G4) is deleted. If necessary, save configuration file manually before **Proxy server** upgrading.
2. To start the upgrade process, execute the following command:
   `sh ./<distribution_file>.run`
3. If necessary, replace the `drwcsd-proxy.xml` configuration file with the file saved before the upgrade process.

Index

A

Active Directory
- Agent, installing 46
- Agent, uninstalling 57

Agent
- installing 30
- installing, Active Directory 46
- installing, remote 43, 46
- uninstalling 55, 57

anti-virus network
- planning 21

anti-virus package
- installing 30, 46
- uninstalling 55

anti-virus Server
- installing, for Unix 27
- uninstalling, for UNIX 53
- uninstalling, for Windows 55
- upgrading, for UNIX OS 61
- upgrading, for Windows OS 58

C

components
- uninstalling 55

creating
- user account 34

D

demo key files 20

distribution kit 18

Dr.Web Agent
- installing 30
- installing, Active Directory 46
- installing, remote 43, 46
- uninstalling 55, 57

Dr.Web Browser-Plugin
- installing 28
- uninstalling, for UNIX 54
- uninstalling, for Windows 55

Dr.Web Server
- installing, for Unix 27
- uninstalling, for UNIX 53
- uninstalling, for Windows 55
- upgrading, for UNIX OS 61
- upgrading, for Windows OS 58

Dr.Web Server extra package
- removing for UNIX 54

Dr.Web Server removing
- extra packagre, for UNIX 54

I

icons
- network scanner 44

installing
- Agent 30, 34
- Agent, Active Directory 46
- Agent, remote 43, 46
- anti-virus Server 27
- Dr.Web Browser-Plugin 28
- NAP Validator 50
- proxy Server 50

K

key files 19
- demo 20
- receiving 19
- see also registration 19

L

licensing 19

N

NAP Validator
- installing 50

Network
- Scanner 43

P

proxy server
- installing 50
- uninstalling 57
- updating 67

R

registration
- Dr.Web product 19

S

Scanner
- Network 43

station

Index

station
user account, creating 34
system requirements 14

U

uninstalling
Agent 55
Agent, Active Directory 57
anti-virus package 55
anti-virus Server 53, 55
Dr.Web Browser-Plugin 54, 55
proxy server 57
updating
Dr.Web ESS 58
proxy server 67
upgrading
Server, for UNIX OS 61
Server, for Windows OS 58
user account
station, creating 34

© Doctor Web, 2015